

UNIVERSIDAD AUTÓNOMA DE MADRID

TRABAJO DE FIN DE MÁSTER

---

# The field of moduli and fields of definition of dessins d'enfants

---

*Author:*

Moisés HERRADÓN CUETO

*Advisor:*

Andrei JAIKIN ZAPIRAIN

MSC: 11G32, 14H57

Keywords: Dessins d'enfants, algebraic curves, field of definition, field of moduli

June 20, 2014

### Abstract

We introduce dessins d'enfants from the various existing points of view: As topological covering spaces, as surfaces with triangulations, and as algebraic curves with functions ramified over three points. We prove Belyi's theorem that such curves are defined over number fields, and define the action of the Galois group  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  on dessins d'enfants. We prove that several kinds of dessins d'enfants are defined over their field of moduli: regular dessins, dessins with no nontrivial automorphisms and dessins with one face. In the last part, we give two examples of regular dessins d'enfants with a field of moduli that is not an abelian extension of  $\mathbb{Q}$ . Both of the examples have genus 61 and field of moduli  $\mathbb{Q}(\sqrt[3]{2})$ .

### Resumen

Introducimos los dessins d'enfants desde los distintos puntos de vista existentes: como espacios recubridores, como superficies con triangulaciones y como curvas algebraicas con funciones ramificadas sobre tres puntos. Probamos el teorema de Belyi, que dice que tales curvas se pueden definir sobre cuerpos de números, y definimos la acción del grupo de Galois  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  sobre los dessins. Probamos que varios tipos de dessins d'enfants están definidos sobre su cuerpo de moduli: los dessins regulares, los que no tienen automorfismos no triviales, y los que sólo tienen una cara. En la última parte, damos dos ejemplos de dessins d'enfants regulares con cuerpo de moduli que no es una extensión abeliana de  $\mathbb{Q}$ . Ambos ejemplos tienen género 61 y cuerpo de moduli  $\mathbb{Q}(\sqrt[3]{2})$ .

# Introduction

There are many ways to define dessins d'enfants. The first one is as a compact orientable surface with a graph embedded in it, such that its vertices can be bicolored, and the faces are homeomorphic to disks. From here, one can divide the surface in triangles, by choosing a point on each face and joining it to the vertices of the face. Using these triangles, one can then define a covering map from the surface onto the sphere, by dividing the sphere into two triangles (the hemispheres) and then mapping the triangles in the original surface to the ones in the sphere. For example, one could proceed like this:

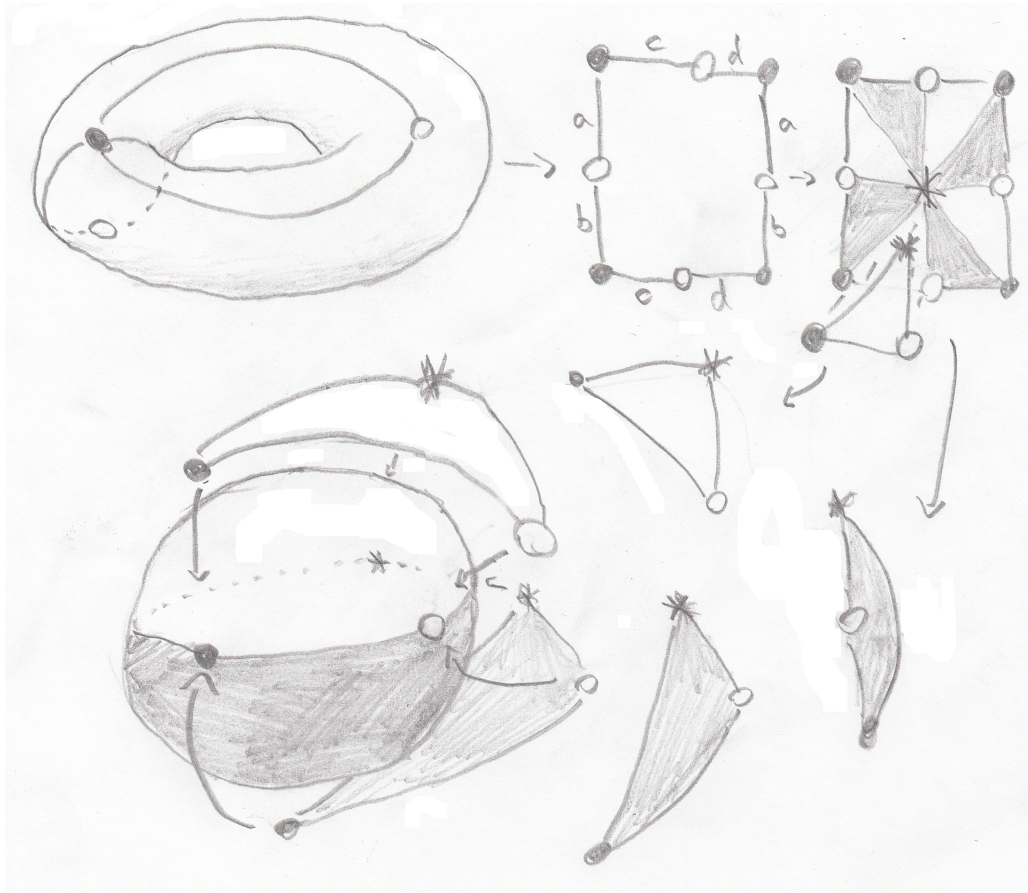


Figure 1: The graph on the torus gives rise to a triangulation. We can then chop the torus up into 8 triangles and produce a 4-sheeted covering of the sphere.

The fun part starts when one takes the complex structure that comes from seeing the sphere as  $\mathbb{P}^1(\mathbb{C})$ , and realizes that this structure determines a complex structure on the surface, i.e. it makes it into a Riemann surface. Also, every compact Riemann surface is isomorphic to some complex algebraic curve, so each dessin d'enfant can be interpreted as a covering, and this covering is actually a morphism of algebraic curves, so it can all be interpreted algebraically. What we end up obtaining is a bijection between dessins d'enfants and complex algebraic curves with a map to  $\mathbb{P}^1(\mathbb{C})$  that is ramified over  $\{0, 1, \infty\}$ , which is called a Belyi map. For example, if we lift the conformal structure to the torus in figure 1, we obtain the plane curve with equation  $y^2 = x^3 - x$ , and the covering map is the map  $(x, y) \mapsto x^2$ .

There's more: these equations that determine the algebraic curves and the functions can actually be written with coefficients not in  $\mathbb{C}$ , but in  $\mathbb{Q}$ . This is one part of what is called Belyi's theorem. The other part, which

Belyi proved in 1980 in [1], is that every curve defined over the algebraic numbers has maps that are ramified over three points. This theorem profoundly impressed Grothendieck, and led him to define *dessins d'enfants*, which he introduced in his *Esquisse d'un Programme* [10].

The interest of *dessins d'enfants* lies in that we have simple combinatorial objects which are equivalent to curves with maps over  $\overline{\mathbb{Q}}$ . Given a curve and a Belyi map, we can take  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  and make it act on the coefficients of their defining equations. What we obtain is sometimes a different *dessin d'enfant*. In fact, the action of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  on the set of *dessins* is faithful, that is, there are no Galois automorphisms that fix every *dessin d'enfant*. Thus, *dessins d'enfants* can be a tool for studying  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . Actually, one can use *dessins d'enfants* to embed  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  into other groups, like  $\text{Out}(\widehat{F}_2)$  or  $\text{Aut}(\widehat{F}_2)$ .

In this work I have tried to present *dessins d'enfants* for someone with my own background. This means a really poor background in algebraic geometry, some algebra, but enough knowledge of group theory, covering spaces and Galois theory of finite extensions. The main criterion I have followed when choosing which proofs to include, and which approach to take, was based on my own background. From my point of view, a great part of the beauty of *dessins d'enfants* is that they are related to many different areas, such as algebraic geometry, complex geometry, topology, group theory, Galois theory and number theory. Thus, many results, especially in Part 1, can be proven using several of the points of view one can use in *dessins d'enfants*. I have no doubt that the reader with some knowledge of algebraic geometry will find many propositions trivial, had I not wandered around trying to prove it using groups. On the plus side, for me, and hopefully for readers with similar background as me, this thesis has meant that I have seen many theorems in algebraic geometry and I have been able to understand them and prove them using techniques that I already know and understand (although at the cost of proving them in a very specific setting). Despite the lack of generality, I think this has given me some great “feel” of algebraic geometry, especially for things like the étale fundamental group, and object which, at the time of writing, I do not know how to define.

With this in mind, in Part 1 there are the different definitions of *dessins d'enfants*, and the proof for the equivalence between them, in an order which I personally find natural. There are many expositions of this, so the reader can try Pierre Guillot's survey [11] for a combinatorics-based approach, or Gironde and González's book [7] for an approach from Riemann surfaces, where one can also find the uniformization approach, which is really fruitful and isn't included here. Another great reference is the book by Lando and Zvonkin [13]. In the next part, the Galois action on *dessins d'enfants* is defined, and we prove Belyi's Theorem. We prove the “obvious” part like [7], which helps us to avoid hardcore algebraic geometry concepts like the ones used in Weil's paper [23]. Then, we define the embedding of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  in  $\text{Aut}(\widehat{F}_2)$  and  $\text{Out}(\widehat{F}_2)$ , and the field of moduli and the field of definition of a *dessin*.

The field of moduli of a *dessin* is the fixed field of the subgroup of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  that leaves it invariant, and a field of definition is a number field such that the *dessin* can be given by equations with coefficients in this number field. Our main problem is, what is the relationship between these fields? It is clear that the field of moduli will be contained in any field of definition. However, the field of moduli isn't always a field of definition. We prove some cases where the field of moduli is the field of definition. It follows from Weil's result, and it can be seen in [24] for *dessins d'enfants*, that regular *dessins d'enfants*, that is, *dessins d'enfants* whose automorphism group acts transitively on the edges, and *dessins d'enfants* without nontrivial automorphisms are both defined over their fields of moduli. Also, it is known (see [13]) that *dessins* that are trees on the sphere are defined over their field of moduli. I present a proof of the slight generalization that *dessins* with one face, on any surface, can be defined over their field of moduli. This proof is due to my advisor, Andrei Jaikin.

In the last part, we turn our attention to the problem of finding a regular *dessin* whose field of moduli is not an abelian extension, which appears in [2]. We construct one example of such a *dessin*, and we use it to give examples of the points of view explained in parts 1 and 2. Also, we show that the curve we construct has itself the same field of moduli. Finally, we comment on another example of a regular *dessin* with non abelian field of moduli that appeared in [21] and [14].

I am grateful to my advisor, Andrei Jaikin, for many insightful discussions, which I have struggled to follow but I have finally learned a lot from them. I also want to thank my friends, girlfriend and family for virtually everything.

My master's degree has been supported by the program Posgrado de Excelencia Internacional of the Autonomous University of Madrid.

# Contents

<b>1</b>	<b>Various definitions of dessins d'enfants</b>	<b>7</b>
1.1	Dessins as covering maps and as holomorphic maps . . . . .	7
1.2	Dessins as algebraic curves and as field extensions . . . . .	9
1.3	Monodromy and automorphisms . . . . .	11
1.4	(Children's) Drawings on surfaces . . . . .	13
1.5	Regular dessins . . . . .	15
1.6	The field $\mathcal{K}$ . . . . .	18
1.6.1	Galois theory of infinite extensions . . . . .	20
1.6.2	Back to $\mathcal{K}$ . . . . .	23
<b>2</b>	<b>The Galois action on dessins d'enfants and Belyi's theorem</b>	<b>25</b>
2.1	The Galois action . . . . .	25
2.2	Belyi's theorem . . . . .	29
2.2.1	Curves defined over the algebraic numbers have Belyi maps . . . . .	29
2.2.2	Curves with Belyi functions are defined over $\overline{\mathbb{Q}}$ . . . . .	31
2.3	The action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\widehat{F}_2$ . . . . .	34
2.3.1	The field of moduli and fields of definition . . . . .	37
2.4	Dessins with one face . . . . .	41
2.5	A dessin that is not defined over its field of moduli . . . . .	45
<b>3</b>	<b>A regular dessin whose field of moduli is <math>\mathbb{Q}(\sqrt[3]{2})</math></b>	<b>47</b>
3.1	A dessin $D_0$ over an elliptic curve . . . . .	47
3.2	The cartographic group of $\widetilde{D}_0$ . . . . .	50
3.3	The dessins conjugate to $\widetilde{D}_0$ . . . . .	51
3.4	Another dessin with non-abelian field of moduli . . . . .	54
3.5	The field of moduli of the underlying curve . . . . .	60
3.6	A different example . . . . .	64



# Part 1

## Various definitions of dessins d'enfants

### 1.1 Dessins as covering maps and as holomorphic maps

There are many equivalent ways to define dessins d'enfants. We are going to give definitions closely related to the ones in [11], which come from the theory of covering spaces and combinatorics. We are going to eventually see that dessins can also be defined as algebraic curves defined over the algebraic numbers with a choice of a meromorphic function with some conditions. To do this from the point of view of topology, we will always see the sphere as the projective complex line  $\mathbb{P}^1 = \mathbb{P}^1(\mathbb{C})$ .

**Definition 1.1.1.** Let  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$  be the sphere with three points removed. A **dessin d'enfant** is a connected covering  $\varphi : S \longrightarrow \mathbb{P}^1 \setminus \{0, 1, \infty\}$  of finite degree.

For example, the identity map of the sphere minus three points is a dessin, which we call the trivial dessin. We can add more structure to a dessin d'enfant: we can give the sphere a complex structure, since we can see it as  $\mathbb{P}^1$ . Then, a complex structure on the sphere determines a complex structure on the covering surface. This complex structure in the sphere isn't affected by our choice of three points  $\{0, 1, \infty\}$ , since the Möbius transformation  $z \mapsto \frac{z-z_0}{z-z_\infty} \frac{z_1-z_\infty}{z_1-z_0}$  sends any three points  $\{z_0, z_1, z_\infty\}$  to  $\{0, 1, \infty\}$  and it is biholomorphic.

So a dessin is equivalent to choosing a covering of  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ , which will be holomorphic once we pick a suitable complex structure in the covering surface. Now, the key observation is that one can compactify the covering surface and extend the covering map  $\varphi$  to produce a holomorphic map from a compact Riemann surface into the Riemann sphere.

**Proposition 1.1.2.** *cubierta* Let  $\varphi : S \longrightarrow \mathbb{P}^1 \setminus \{0, 1, \infty\}$  be a dessin d'enfant. There exists a compact Riemann surface  $\bar{S}$  and a holomorphic map  $\bar{\varphi} : \bar{S} \longrightarrow \mathbb{P}^1$ , such that

1.  $S$  is an open set of  $\bar{S}$ .
2.  $\bar{S} \setminus S$  is a finite set.
3.  $\bar{\varphi}|_S = \varphi$ .
4. All the ramification points of  $\bar{\varphi}$  lie in the preimage of  $\{0, 1, \infty\}$ .

And any other compact Riemann surface  $\bar{S}'$  with a map  $\bar{\varphi}' : \bar{S}' \longrightarrow \mathbb{P}^1$  satisfying the same conditions is biholomorphic to  $\bar{S}$ , by a biholomorphism  $\Psi$  such that  $\bar{\varphi}' = \bar{\varphi} \circ \Psi$ .

*Proof.* There is an obvious complex structure on  $S$ , defined as follows: for each point  $p \in S$ , let  $U$  be a simply connected neighborhood of  $\varphi(p)$ . Now, since  $U$  is simply connected and  $\varphi$  is a covering map,  $\varphi^{-1}(U)$  will be a finite disjoint union of open sets homeomorphic to  $U$ . Let  $U_p$  be the one containing  $p$ .  $\varphi|_{U_p}$  is a homeomorphism, and therefore we have a chart  $(U_p, \varphi|_{U_p})$ . Any two of these charts are compatible, since the transition maps between different charts are always the identity maps of some sets of  $\mathbb{P}^1$ .

We need to add some points to  $S$  now in order to compactify it. Let us build the preimage of 0. Let  $U$  be the punctured disc of radius 1/2 around 0. If we restrict  $\varphi$  to the preimage of  $U$ , which is an open set of  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ , it will also be a covering. Therefore, we can split  $\varphi^{-1}(U)$  into its connected components, which are open, since  $S$  is locally connected (it is a surface, after all). Let these connected components be  $U_1, \dots, U_m$ . For each  $i$ ,  $\varphi_i = \varphi|_{U_i}$  is a covering map of  $U$ . Now,  $U$  has the homotopy type of a circle, and every covering of a circle is of the form  $z \mapsto z^n$  for some  $n \in \mathbb{Z} \setminus \{0\}$ . Via the homotopy equivalence between the circle and  $U$ , the covering of the circle is equivalent to the map  $z \mapsto 2^{n-1}z^n$ . This means that there is a homeomorphism  $\psi : U_i \longrightarrow U$  such that the following diagram commutes:

$$\begin{array}{ccc}
U_i & \xrightarrow{\psi} & U \\
& \searrow \varphi_i & \swarrow \pi = z \mapsto 2^{n-1}z^n \\
& & U
\end{array}$$

i.e.  $\varphi_i = \pi \circ \psi$ . Now, we can take  $\bar{U} = U \cup \{0\}$  and define a point  $p_i = \psi^{-1}(0) \in U_i$ , such that  $\bar{U}$  and  $\bar{U}_i = U_i \cup \{p_i\}$  are homeomorphic by a homeomorphism  $\bar{\psi}$  extending  $\psi$ . Also, we can use  $(\bar{U}_i, \bar{\psi}^{-1})$  as a chart around  $p_i$ . This chart is compatible with the atlas previously defined: If we have another point  $q$ , with a neighborhood  $V_q$  which maps homeomorphically to  $V$ , the transition map is  $\varphi|_{U_p} \circ \psi^{-1}$ . Now, since  $\varphi_i = \pi \circ \psi$ , when we restrict ourselves to the intersection of the charts, we have that  $\varphi|_{U_p} \circ \psi^{-1} = \pi$ , which is holomorphic.

Finally, if we define  $\bar{\varphi}(p_i) = 0$  for all these new points, the resulting map is holomorphic, because we have defined it to be (if we take charts, the map will be  $z \mapsto z^n$  for some  $n$ , on every chart). We can do the same thing to define preimages of 1 and  $\infty$  (using disjoint neighborhoods of 1 and  $\infty$ ), and we end up adding a finite number of points, obtaining a Riemann surface  $\bar{S}$  and a holomorphic map to  $\mathbb{P}^1$ . Note that, in the topology we have defined every open subset of  $S$  is an open subset of  $\bar{S}$ , so in particular  $S$  is an open subset of  $\bar{S}$ .

Also,  $\bar{S}$  is compact: take an open cover  $\mathcal{U} = \{U_i : i \in I\}$  of  $\bar{S}$ . Each point  $p \in \mathbb{P}^1$ , has a finite number of preimages. Now, for every point  $p \in \mathbb{P}^1$ , there is a neighborhood  $V^p$  such that  $\bar{\varphi}^{-1}(V^p) = \sqcup_{j=1}^m V_j^p$ , and  $\bar{\varphi}|_{V_j^p}$  is conjugate to the map  $z \mapsto z^n$ , in a neighborhood of 0. For each preimage of  $p$ , we can pick a neighborhood contained in its corresponding  $V_p^j$  and some set  $U \in \mathcal{U}$ ; take the images of all these neighborhoods and intersect them. This gives a neighborhood  $U^p$  of  $p$  such that every connected component of its preimage is contained in an element of the cover. Since  $\mathbb{P}^1$  is compact, the covering  $\{V^p\}$  has a finite subcover  $V_1, \dots, V_r$ . Also, the preimage by  $\bar{\varphi}$  of each set  $V_j$  is contained in the union of a finite number of  $U_i$ 's, and so the whole collection of these  $U_i$ 's is the finite subcover we are looking for. So  $\bar{S}$  is compact.

For the uniqueness, note that the complex structure is completely determined on the points of  $S$ , so any two surfaces verifying the proposition will have open sets  $S$  that will be biholomorphic, and whose complements will be finite sets. However, holomorphic functions can be extended to isolated points, so the surfaces will be isomorphic.  $\square$

Throughout this work, if we have a map  $\varphi : S \rightarrow T$ , and a point  $p \in S$ , such that  $\varphi'(p) = 0$ , we will call  $p$  a **ramification point** and  $\varphi(p)$  a **ramification value**. Now, the previous proposition proves that dessins d'enfants can be viewed as holomorphic mappings of compact Riemann surfaces onto the Riemann sphere, such that their ramification values are contained in  $\{0, 1, \infty\}$ . The converse is also true: if one restricts an holomorphic mapping to its unramified points, the result is a covering, because of the open mapping theorem for holomorphic maps. Therefore, from a surface with a map to the sphere ramified over at most three points, one obtains a dessin by removing the ramification points from the surface and  $\{0, 1, \infty\}$  from  $\mathbb{P}^1$ .

We can give dessins even more structure: it is a classical result that every compact Riemann surface is an algebraic curve, that is, it can be embedded (as a nonsingular curve) in  $\mathbb{P}^n(\mathbb{C})$  for some  $n$  (actually  $n = 3$  is enough), such that its image is the zero set of some complex polynomials. This result can be found in [7], assuming the uniformization theorem. The uniformization theorem and its proof can be found in [5]. The result can also be found in [15], if one is willing to assume that Riemann surfaces have enough meromorphic functions.

Every algebraic curve we talk about from now on, unless we say otherwise, is non-singular and projective.

For an algebraic curve  $C$ , we call  $f : C \rightarrow \mathbb{P}^1$  a **Belyi function** if it is ramified over some subset of  $\{0, 1, \infty\}$ . If  $f$  is a Belyi function for  $C$ , we call  $(C, f)$  a **Belyi pair**. What we have established is that dessins d'enfants are equivalent to Belyi pairs. Since we will use equivalent definitions for dessins d'enfants, we might sometimes abuse notation and call a Belyi pair a dessin d'enfant.

There is one last bit of additional structure we can give dessins d'enfants. It is thanks to Belyi's theorem, which says the following: a curve has a Belyi function if and only if it is defined over the field of algebraic numbers. We will talk about dessins d'enfants for a while before proving it, but we are giving the motivation now. If one has a curve given by some set of equations and a Belyi function on it, all of whose coefficients are algebraic numbers one can take an element of  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  and have it act on the coefficients of the equations and the function. This gives a Belyi pair which isn't necessarily isomorphic to the previous one. Thus, we have a non-trivial action of  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ . In fact, this action is faithful in many ways. We will talk a lot about the Galois action after we have finished introducing dessins d'enfants.

We are going to take a moment to talk about the relationship between different dessins. Namely, dessins form a category. When we see dessins as covers of  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ , a morphism between two Belyi pairs  $(C_1, f_1)$  and  $(C_2, f_2)$  is a morphism (of curves, or equivalently, a holomorphic map)  $g : C_1 \rightarrow C_2$  such that  $f_1 = f_2 \circ g$ . We say that the dessin  $(C_1, f_1)$  **covers** the dessin  $(C_2, f_2)$ . Two dessins are equivalent, or isomorphic, if they are isomorphic in this category.



## 1.2 Dessins as algebraic curves and as field extensions

We are going to talk about dessins d'enfants from the point of view of the fields of functions of the algebraic curves involved. We are going to talk about curves over  $\mathbb{C}$ , but we ask the reader to bear in mind that every statement we make about  $\mathbb{C}$ -algebras from now on is also valid for any algebraically closed field of characteristic 0, in particular if one replaces  $\mathbb{C}$  with  $\overline{\mathbb{Q}}$ . This is important, since dessins are defined over  $\overline{\mathbb{Q}}$ , and this will ultimately be the field we are interested in.

If we have a Belyi pair  $(C, f)$ , we can look at its field of functions  $\mathbb{C}(C)$ . To the morphism  $f : C \rightarrow \mathbb{P}^1$  corresponds a field homomorphism  $f^* : \mathbb{C}(t) \rightarrow \mathbb{C}(C)$ , given by  $P \mapsto P(f)$ . This is the same as the field inclusion  $\mathbb{C}(f) \subset \mathbb{C}(C)$ . Thus, to a dessin we can associate an extension of  $\mathbb{C}(t)$ .

Conversely, finite extensions of  $\mathbb{C}(t)$  are always fields of functions of curves.

**Theorem 1.2.1.** *The following categories are equivalent:*

1. *Non-singular projective complex algebraic curves, with non-constant regular functions as morphisms.*
2. *Extensions of  $\mathbb{C}$  of degree of transcendence 1, with  $\mathbb{C}$ -algebra homomorphisms as morphisms.*

*The functor takes curves to their function fields.*

*Proof.* The proof can be found in [7]. We will just state how the functor acts on morphisms: given a regular map (a rational function) between two algebraic curves  $\varphi : C \rightarrow C'$ , one can consider the  $\mathbb{C}$ -algebra homomorphism

$$\begin{aligned} \varphi^* : \mathbb{C}(C') &\longrightarrow \mathbb{C}(C) \\ f &\longmapsto \varphi^* f = f \circ \varphi \end{aligned}$$

Note that such morphisms are always injective, since both algebras are fields. Conversely, if one has an embedded algebraic curve  $C'$  with homogeneous coordinates  $(Y_0 : \dots : Y_n)$  (which can be seen as functions on the curve) and a homomorphism  $\varphi^* : \mathbb{C}(C') \rightarrow \mathbb{C}(C)$ , it is associated to the map

$$\begin{aligned} \varphi : C &\longrightarrow C' \\ (X_0 : \dots : X_m) &\longmapsto (Z_0 : \dots : Z_n) = (\varphi^*(Y_0) : \dots : \varphi^*(Y_n)) \end{aligned}$$

□

From here follows that, since dessins d'enfants are certain morphisms from curves onto  $\mathbb{P}^1$ , via this equivalence, they must correspond to some extensions of the field of functions of  $\mathbb{P}^1$ , which is  $\mathbb{C}(t)$ . In order to speak about ramification of points in field extensions, we first need a way to speak about points in the context of a field. The way to do this is via the valuations of the field of functions.

**Definition 1.2.2.** Let  $K$  be a field. A (discrete) **valuation** on  $K$  is a non-zero map  $\nu : K^\times \rightarrow \mathbb{Z}$  such that

- $\nu(ab) = \nu(a) + \nu(b) \ \forall a, b \in K^\times$
- $\nu(a + b) \geq \min\{\nu(a), \nu(b)\} \ \forall a, b \in K^\times$
- If  $k$  is a subfield of  $K$ , and  $\nu(k^\times) = 0$ , we say that  $\nu$  is a  $k$ -valuation.

One usually extends a valuation to the whole field by setting  $\nu(0) = +\infty$ .

From the second property it follows that if  $\nu(a) \neq \nu(b)$ , then  $\nu(a + b) = \min\{\nu(a), \nu(b)\}$ , for if  $\nu(a) < \nu(b)$  and  $\nu(a) < \nu(a + b)$ , then  $\nu(a) = \nu(a + b - b) < \min\{\nu(a + b), \nu(-b)\}$ .

It is easy to assign a  $\mathbb{C}$ -valuation to a point on a curve. One can take, for each function  $f \in \mathbb{C}(C)$ , the order at a point  $P$  (which is either the order of the zero if  $f(P) = 0$ , or minus the order of the pole if  $f$  has a pole at  $P$  or 0 if  $f$  neither has a zero nor a pole). It is straightforward to check that  $f \mapsto \text{ord}_P(f)$  is a  $\mathbb{C}$ -valuation. There are other valuations associated to  $P$ , since  $m \cdot \text{ord}_P$  for any  $m \in \mathbb{N}$  is also a valuation. If two valuations differ by multiplication by a constant, we say that they are equivalent. If one asks for valuations to be surjective, every  $\mathbb{C}$ -valuation corresponds to a point:

**Proposition 1.2.3.** *Let  $\mathbb{C}(C)$  be the field of functions of an algebraic curve. Then, the following sets are in bijective correspondence:*

- *The points in  $C$ .*
- *The surjective  $\mathbb{C}$ -valuations of  $\mathbb{C}(C)$ .*

And the correspondence is given by  $P \mapsto \text{ord}_P$ .

*Proof.* The proof can be found in Proposition 3.17 of [7].  $\square$

From now on, by “valuation” we will mean “discrete  $\mathbb{C}$ -valuation”.

If we have a morphism between two curves  $\varphi : C \rightarrow C'$ , the morphism also maps valuations to valuations. By the chain law, for any function  $f \in \mathbb{C}(C')$  and any point  $P \in C$ ,

$$\text{ord}_P(\varphi^* f) = \text{ord}_P(f \circ \varphi) = \text{ord}_{\varphi(P)}(f) e_P(\varphi)$$

Where  $e_P(\varphi)$  is the ramification index of  $\varphi$  at  $P$ , i.e. the order of the zero of  $\varphi$  at the point  $P$ , or the order with which the derivative of  $\varphi$  vanishes at  $P$  plus 1.

This can give us the idea to define a map of valuations: for a valuation  $\nu$  of  $\mathbb{C}(C)$ , one can define

$$\varphi(\nu) \sim \nu \circ \varphi^*$$

Where by  $\sim$  we mean equal up to multiplication by a constant. Therefore, for every point  $P$ , we have

$$\varphi(\text{ord}_P) = e_P(\varphi) \text{ord}_{\varphi(P)}$$

Since the valuation  $\text{ord}_{\varphi(P)}$  is surjective, one can use this to define the ramification of a point by a  $\mathbb{C}$ -algebra homomorphism, and as we have just seen, it will match our previous definition of ramification.

**Definition 1.2.4.** Let  $\varphi^* : \mathbb{C}(C') \rightarrow \mathbb{C}(C)$  be a morphism between fields of functions. For every valuation  $\nu$  of  $\mathbb{C}(C)$ , we define its image  $\varphi(\nu)$  as the unique valuation of  $\mathbb{C}(C')$  such that there exists a natural number  $e_\nu(\varphi)$  with

$$\nu \circ \varphi^* = e_\nu(\varphi) \varphi(\nu)$$

We call  $e_\nu(\varphi)$  the order of ramification of  $\varphi$  at the point  $\nu$ .

Note that, since  $\varphi^*$  is always injective, we can view  $\mathbb{C}(C')$  as a subfield of  $\mathbb{C}(C)$ . If we do this, then the image of a valuation is just its restriction to the smaller field.

Since we know that valuations and points correspond to each other, we have some facts that we already know about points.

**Proposition 1.2.5.** *Let  $\varphi : C \rightarrow C'$  be a morphism of curves. Then*

1. *The number of valuations  $\nu$  of  $\mathbb{C}(C)$  for which  $e_\nu(\varphi) > 1$  is finite.*
2. *For every valuation  $\nu$  of  $\mathbb{C}(C')$ , the number*

$$\sum_{\varphi(\nu')=\nu} e_{\nu'}(\varphi)$$

*is finite, constant and equal to  $[\mathbb{C}(C) : \varphi^* \mathbb{C}(C')]$ .*

We will not prove or use the last part of the proposition, that the degree of the extension is the degree of the map, but we will prove it for dessins later on, in Proposition 1.5.5.

Back to dessins d'enfants, a finite extension  $\mathbb{C}(t) \subset K$  is the same as a morphism  $i : \mathbb{C}(t) \rightarrow K$ , which corresponds to a morphism of curves  $\varphi : C \rightarrow \mathbb{P}^1$ . Thus, a dessin d'enfant can also be defined as an extension of  $\mathbb{C}(t)$  that is ramified at most over 0, 1 and  $\infty$  (that is, the valuations  $\text{ord}_0$ ,  $\text{ord}_1$  and  $\text{ord}_\infty$ ).

**Proposition 1.2.6.** *The category of dessins d'enfants, with coverings as morphisms, is equivalent to the category of finite extensions of  $\mathbb{C}(t)$  unramified outside of  $\{0, 1, \infty\}$ , with homomorphisms of extensions as morphisms.*

*Proof.* We have already seen the proof of everything, aside from identifying the morphisms. If we have a morphism between two dessins, which we see as Belyi functions  $f : C \rightarrow \mathbb{P}^1$  and  $f' : C' \rightarrow \mathbb{P}^1$ , a morphism is a rational function  $\varphi : C \rightarrow C'$  such that  $f' \circ \varphi = f$ . If we take the functor which maps curves to their fields of functions, this becomes  $\varphi^* \circ f'^* = f^*$ , and if we see  $f^*$  and  $f'^*$  as inclusions of  $\mathbb{C}(t)$  in the respective fields of functions, then this condition precisely means that  $\varphi^*$  preserves  $\mathbb{C}(t)$ . In other words, it is a homomorphism of extensions of  $\mathbb{C}(t)$ .  $\square$

### 1.3 Monodromy and automorphisms

In this section, we will see yet more characterizations of dessins d'enfants. It all boils down to the classification of covering spaces from topology. Results from this section can be found in Munkres' Topology [16], in chapter 13. All coverings we will speak about will be connected.

Recall that, from a continuous map  $f : X \rightarrow Y$  such that  $f(x_0) = y_0$ , there is a homomorphism of the spaces' fundamental groups, called  $f_*$ , and it is given by  $\gamma \mapsto f \circ \gamma$ .

**Proposition 1.3.1** (Lifting lemma). *Let  $p : C \rightarrow X$  be a covering map, where  $X$  is a locally path connected topological space. Let  $Y$  be a locally path connected and path connected topological space and  $f : Y \rightarrow X$  be a continuous map. Choose points  $c_0 \in C$ ,  $x_0 \in X$  and  $y_0 \in Y$  such that  $p(c_0) = x_0$  and  $f(y_0) = x_0$ . Then, we define a **lifting**  $\tilde{f}$  of  $f$  to  $C$  to be a map  $\tilde{f} : Y \rightarrow C$  such that the following diagram commutes and  $\tilde{f}(y_0) = c_0$*

$$\begin{array}{ccc} & C & \\ & \downarrow p & \\ Y & \xrightarrow{f} & X \end{array} \quad \begin{array}{c} \nearrow \tilde{f} \\ \nearrow f \end{array}$$

*Such a lifting exists if and only if  $f_*(\pi_1(Y, y_0)) \subset p_*(\pi_1(C, c_0))$ . If the lifting exists, it is unique.*

*Proof.* This is lemma 79.1 in Munkres' text [16]. □

Thus, for a covering with a base point  $p : (C, c_0) \rightarrow (X, x_0)$ , the group  $p_*(\pi_1(C, c_0))$  plays a very important role. This is why we call it **the subgroup associated to the covering** (note that it depends on the choice of a base point). The other main result is the following: for nice enough spaces, to every subgroup corresponds a covering.

**Proposition 1.3.2.** *Let  $X$  be semi-locally simply connected (for example, let  $X$  be a manifold), with a fixed base point  $x_0$ . Then, for every subgroup  $H < \pi_1(X, x_0)$ , there exists a covering  $p : C \rightarrow X$  such that  $p_*(\pi_1(C, c_0)) = H$*

*Proof.* This is theorem 82.1 in [16]. □

From the lifting lemma, it follows that the covering associated to a subgroup is unique, up to isomorphism. For two coverings  $p_1 : (C_1, c_1) \rightarrow (X, x_0)$  and  $p_2 : (C_2, c_2) \rightarrow (X, x_0)$ , we define a morphism between them to be a map  $\varphi : C_1 \rightarrow C_2$  such that  $p_1 = p_2 \circ \varphi$ , as we did with dessins. A morphism with base points is the same with the additional condition that  $\varphi(c_1) = c_2$ .

**Proposition 1.3.3.** *Let  $p_1 : (C_1, c_1) \rightarrow (X, x_0)$  and  $p_2 : (C_2, c_2) \rightarrow (X, x_0)$  be two coverings, with associated subgroups  $H_1$  and  $H_2$ , respectively. Then, there exists a morphism with base points from  $C_1$  to  $C_2$  if and only if  $H_1 < H_2$ . If it exists, it is unique.*

*Proof.* A morphism with base points is the same as a lifting of the map  $p_1$  to the covering  $p_2$ . With this in mind, it follows from the lifting lemma. □

**Corollary 1.3.4.** *Two covering spaces with the same associated subgroup are isomorphic with base points.*

We want to remove the base point, and to see when two coverings are isomorphic regardless of the base point. If two coverings are isomorphic, then they must be isomorphic with a suitable choice of base points. Now, if we have a covering  $p : (C, c_0) \rightarrow (X, x_0)$ , and we choose another point  $c_1$  such that  $p(c_1) = x_0$ , we know that  $\pi_1(C, c_0)$  and  $\pi_1(C, c_1)$  are related in the following way: if we choose a path  $\eta$  from  $c_0$  to  $c_1$ , then  $\pi_1(C, c_1) = \eta * \pi_1(C, c_0) * \eta^{-1}$ , where  $*$  denotes path concatenation. We can apply  $p_*$  to the previous relation, and  $p_*(\eta)$  will be a loop, since  $p(c_0) = p(c_1)$ . Therefore,  $H_1 = p_*(\eta)H_2p_*(\eta)^{-1}$ .

**Proposition 1.3.5.** *Let  $p_1 : (C_1, c_1) \rightarrow (X, x_0)$  and  $p_2 : (C_2, c_2) \rightarrow (X, x_0)$  be two coverings, with associated subgroups  $H_1$  and  $H_2$ . There exists a morphism of coverings  $\varphi : C_1 \rightarrow C_2$  that doesn't preserve the base points if and only if  $H_1 \subset gH_2g^{-1}$  for some  $g \in \pi_1(X, x_0)$ .*

*Proof.* Suppose there is such a morphism. Then, if  $c'_2 = \varphi(c_1)$ ,  $\varphi$  is a morphism from  $(C_1, c_1)$  to  $(C_2, c'_2)$  that does preserve the base points. Therefore,  $H_1$  is contained in the subgroup associated to  $(C_2, c'_2)$ . But changing the base point of a covering space gives a conjugate subgroup, so we have what we want:  $H_1 \subset gH_2g^{-1}$ .

Conversely, suppose that  $H_1 \subset gH_2g^{-1}$ . Pick a loop  $\eta$  whose class in the fundamental group of  $X$  is  $g^{-1}$ . We can lift this path to  $C_2$ , starting from  $c_2$  (by the lifting lemma). Call  $c'_2$  the endpoint of the lifted path. Then, by what we seen before the proposition, the subgroup associated to  $(C_2, c'_2)$  is  $gH_2g^{-1}$ . Therefore, there exists a morphism from  $(C_1, c_1)$  to  $(C_2, c'_2)$ , which can be seen as a morphism to  $(C_2, c_2)$  that doesn't preserve the base points. □

**Corollary 1.3.6.** *Two covering spaces are isomorphic if and only if their associated subgroups are conjugate.*

We are seeing that the subgroups of the fundamental group and the coverings of a space are closely related. Another way of seeing this relation is the **monodromy action**. Given a covering space  $p : C \rightarrow (X, x)$ , let  $F = p^{-1}(\{x\})$ . We can make  $\pi_1(X, x)$  act on  $F$  on the following way: take a loop  $\eta$  in  $\pi_1(X, x)$  and  $c \in F$ . As we did in the proof of the previous proposition, lift it to a path  $\tilde{\eta}$  in  $C$  so that it starts on  $c$ . Then, call  $\eta(c) = \eta(1)$ . It is easy to check that this doesn't depend of the homotopy class of  $\eta$ . Also, it is indeed an action of  $\pi_1(X, x)$  on  $F$ : if we have two loops  $\eta$  and  $\gamma$ , the action of  $\eta$  followed by the action of  $\gamma$  is clearly the same as the action of  $\eta * \gamma$ . Thus, we have a right action. It is also transitive, since  $C$  is path connected.

Also, note that  $\eta(c) = c$  if and only if  $\eta$  lifts to a loop  $\tilde{\eta}$  in  $C$ . This means in turn that  $\eta = p_*(\tilde{\eta}) \in p_*(\pi_1(C, c))$ . Therefore, the stabilizer of the point  $c$  by the monodromy action is the subgroup associated to  $(C, c)$ . Since we have a transitive action, the fiber  $F$  of  $x$  is in bijection with  $H \backslash \pi_1(X, x)$ , where  $H$  is the subgroup associated to  $(C, c)$ . In particular, the degree of the covering, which is the cardinality of  $F$ , is equal to the index of  $H$  in  $\pi_1(X, x)$ .

This gives two ways to look at a covering: as a conjugacy class of subgroups, and as a transitive  $\pi_1(X, x)$ -action. We can apply this to dessins: we are looking at covers of  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ , and the fundamental group of  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$  is  $F_2$ , the free group on two generators. A dessin can also be seen as the conjugacy class of a finite index subgroup of  $F_2$ . We will fix  $1/2 \in \mathbb{P}^1$  as the base point and we will pick two canonical generators for this group:  $x$ , which can be parametrized as  $t \mapsto \frac{1}{2}e^{2\pi it}$ , and  $y$ , which is  $t \mapsto 1 - \frac{1}{2}e^{2\pi it}$ . In other words,  $x$  goes around 0 and  $y$  goes around 1.

Dessins are in correspondence with conjugacy classes of subgroups of  $F_2$  of finite index. Also, if one takes the monodromy action, a dessin can also be seen as a transitive right action of  $F_2$  on a finite set.

From the fact that dessins are equivalent to (right)  $F_2$ -actions, we can give yet another definition, which consists of, given an action, consider the induced morphism  $f : F_2 \rightarrow S_F$  on the group of permutations of  $F$  (which we see as also acting on the right on  $F$ ). Then, a dessin can be seen as a homomorphism from  $F_2$  to  $S_n$  such that its image is a transitive subgroup of  $S_n$ . Dessins are equivalent if these morphisms are conjugate in  $S_n$ . The subgroup associated to the cover is then the preimage of the stabilizer of any point (since all the stabilizers are conjugate). Given a dessin, we call the image of  $F_2$  in a permutation group the **cartographic group** of the dessin.

With the point of view of actions, morphisms between dessins are as follows: if one has a dessin  $(C, f)$  and the transitive action of  $F_2$  on the fiber  $X$  given by the monodromy, and we have a morphism to another dessin  $(C', f')$ , we can consider a base point in  $C$  and its image in  $C'$ , which gives an inclusion between a group  $H$  associated to  $(C, f)$  and a group  $H'$  associated to  $(C', f')$ . Then,  $X \cong H \backslash F_2$ , and  $H$  is contained in  $H'$ , so  $H'$  is the union of some cosets of  $H$ . Therefore, the cosets of  $H'$  form a partition of  $H \backslash F_2$ . In the set  $X$ , we are just quotienting by the relation  $a \sim b \Leftrightarrow \exists h \in H' : a^h = b$ . This quotient is simply  $H' \backslash F_2$ , so  $F_2$  acts on it by the induced action, given by  $[a]^g = [a^g]$ . Thus, a morphism between actions is a map  $\varphi : X \rightarrow X'$  that commutes with the action of  $F_2$ , that is,  $\varphi(x^g) = \varphi(x)^g$ . Since we are requiring all actions to be transitive, such a map will be surjective.

Finally,  $F_2$  is a special group, since it satisfies a universal property: for every group  $G$  and every two elements  $\bar{x}, \bar{y} \in G$ , there exists a unique homomorphism  $\pi : F_2 \rightarrow G$  such that  $\pi(x) = \bar{x}$  and  $\pi(y) = \bar{y}$ . For a subgroup  $H < F_2$ , we can consider the biggest normal subgroup contained in it, which is called the core, and it is  $\text{Core}_{F_2} H = \bigcap_{g \in F_2} g^{-1} H g$  (which is of finite index, bounded by  $[F_2 : H]!$ ), we can consider the map  $\pi : F_2 \rightarrow F_2 / \text{Core}_{F_2} H$ . This gives a homomorphism from  $F_2$  onto a group  $G$  with a distinguished subgroup,  $\pi(H)$ , that satisfies that  $\text{Core}_G \pi(H) = 1$ . Conversely, given a group  $G$  with two generators  $\bar{x}, \bar{y}$ , and a subgroup  $\bar{H}$  such that  $\text{Core}_G \bar{H} = 1$ , there is a subgroup  $H$  of  $F_2$  and a map  $\pi$  taking  $H$  to  $\bar{H}$  and the generators of  $F_2$  to  $\bar{x}, \bar{y}$ .

To sum up:

**Proposition 1.3.7.** *Dessins d'enfants are in correspondence with the following sets:*

1. *The finite index subgroups of  $F_2$ , up to conjugation. A dessin  $C_1$  covers another one  $C_2$  if and only if their corresponding subgroups  $H_1$  and  $H_2$  satisfy that  $H_1 \subset g^{-1} H_2 g$  for some  $g \in F_2$ .*
2. *Finite groups  $G$  with two distinguished generators  $\bar{x}$  and  $\bar{y}$  and a distinguished subgroup  $\bar{H}$ , such that  $\text{Core}_G \bar{H} = 1$ .*

**Proposition 1.3.8.** *The category of dessins d'enfants is equivalent to the following categories:*

1. *Transitive right actions of  $F_2$  on finite sets. A morphism between two sets with  $F_2$  actions is a map  $\varphi : X \rightarrow X'$  such that for all  $g \in F_2$  and every  $x \in X$ ,  $g(\varphi(x)) = \varphi(g(x))$ .*

2. Pairs of permutations  $\bar{x}, \bar{y} \in S_n$  that generate transitive subgroups or, equivalently, morphisms from  $F_2$  to  $S_n$  such that  $x$  and  $y$  are mapped to such generators. A morphism between  $\bar{x}_1, \bar{y}_1 \in S_n$  and  $\bar{x}_2, \bar{y}_2 \in S_m$  is a map  $\varphi : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$  such that  $\varphi \circ \bar{x}_1 = \bar{x}_2 \circ \varphi$ , and  $\varphi \circ \bar{y}_1 = \bar{y}_2 \circ \varphi$ .

## 1.4 (Children's) Drawings on surfaces

We can look at the monodromy in a much more geometric way. Let us consider the following triangulation of the sphere: Take the real line, which is a circle that passes through 0, 1 and  $\infty$ , and make these three points vertices and make the segments the real line is divided in by these points into edges. The hemispheres are two triangles with vertices 0, 1 and  $\infty$ . We will color the triangle with positive imaginary part white, and the other one black.

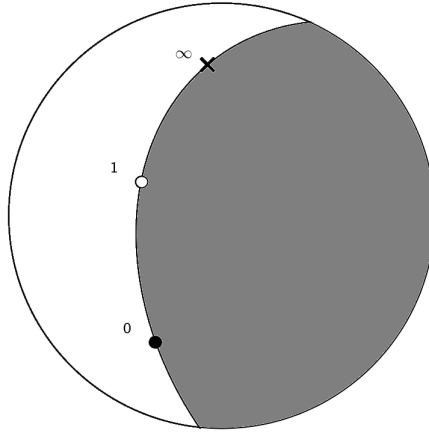


Figure 1.1: The triangulation on the sphere

If we have a dessin d'enfant, the triangulation can be lifted to the covering surface, including the ramification points. We can do this as follows: let  $p : C \rightarrow \mathbb{P}^1$  be the covering map. If we take the white triangle and remove its vertices, we can call it  $T$  and consider the inclusion  $i : T \rightarrow \mathbb{P}^1$ . Now, for every point  $P_j$  in  $p^{-1}(1/2)$ , we can lift the inclusion (by the lifting lemma) to a map  $\tilde{i}_j$  so that  $\tilde{i}_j(1/2) = P_j$ . If we do this for the black triangle as well, we obtain the triangulation of  $C$  except for the ramification points. Note that every triangle and every edge are lifted to as many triangles and edges as the degree of the covering. We take the ramification points as vertices, and, since locally the covering looks like  $z \mapsto z^e$ , each point will have  $2e$  edges around it and  $e$  triangles of each color.

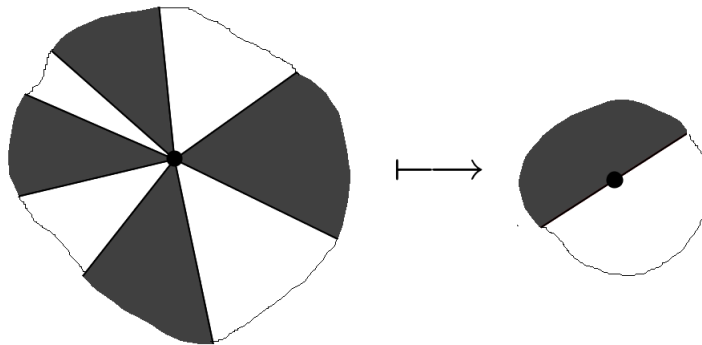


Figure 1.2: A neighborhood of a point with ramification index 4

Thus there is a triangulation on the surface such that every face of it is mapped to a face of the triangulation on  $\mathbb{P}^1$ . We can color the points on  $C$  depending on which image they have. We will say that the preimages of 0 are black points, the preimages of 1 are white points and the preimages of  $\infty$  are stars. We have a surface with a triangulation with vertices of three kinds, and such that each triangle has a vertex of every kind.

We can go the other way round: Start from a triangulated oriented surface with black vertices, white vertices and stars such that each triangle has a vertex of each kind. Since the surface is oriented, for every triangle there is a notion of the counterclockwise order of its vertices. Color each triangle such that the vertices are ordered black-white-star in counterclockwise order white and every other triangle black. Note that this implies that every edge is shared by a triangle of each color. Now, we can map black vertices to 0, white vertices to 1, stars to  $\infty$ , white triangles to the white triangle on the sphere, black triangles to the black triangle on the sphere and edges of triangles to the corresponding segment: this gives a covering of the sphere.

We have proven that dessins are equivalent to triangulated orientable surfaces with three-colored vertices. There is yet another way to represent a dessin: From such a surface, if we delete every star vertex and the edges reaching it, we are left with a bicolored graph embedded in a surface. Each star vertex is a vertex of  $e$  triangles of each color, and when we delete the vertex, these triangles turn into a face with  $2e$  edges. We can also turn this the other way round. If we start with a bicolored graph embedded in an orientable surface, such that the faces are homeomorphic to disks, we can add a star vertex to each face, join it with each vertex on the face and we have a triangulated surface as before. This is the reason why Grothendieck called them dessins d'enfants (children's drawings): because they can just be seen as a drawing on a surface.

From a Belyi function, one can just take the preimage of the segment  $[0, 1]$ , and this will give the graph on the surface.

As an example, we can take the cube dessin on the sphere (we are identifying  $\mathbb{C} \subset \mathbb{P}^1$  with the plane as usual, so every picture has an outer face and a point at infinity):

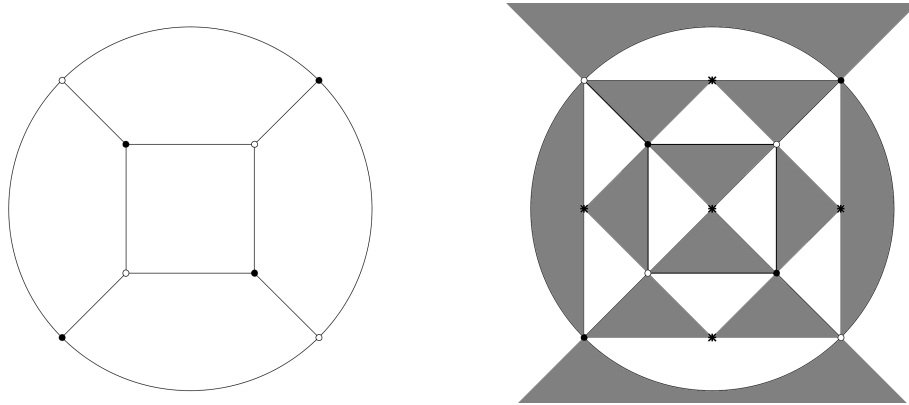


Figure 1.3: The cube with and without the star vertices drawn

Let us take a moment to look at this example from all the points of view we have seen so far. From the triangulated surface, a covering of the sphere is determined. This, in turn, determines a complex structure on the sphere and a holomorphic map. This holomorphic map is given by the equation

$$f(z) = -\frac{1}{12\sqrt{3}} \frac{(z^4 - 2\sqrt{3}z^2 - 1)^3}{z^2(z^4 + 1)^2} = 1 - \frac{1}{12\sqrt{3}} \frac{(z^4 + 2\sqrt{3}z^2 - 1)^3}{z^2(z^4 + 1)^2}$$

We will not stop to see how the equation for the map is obtained. There are techniques for this that can be found in [11] and [13], chapter 2. We can, however, check that this map has degree 12, and that it is invariant under the Möbius transformations

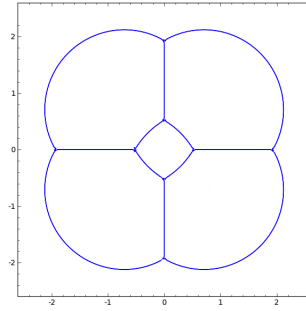
$$z \mapsto -\frac{\sqrt{2}z + 1 + i}{(1 - i)z - \sqrt{2}}, z \mapsto -\frac{\sqrt{2}z + 1 - i}{(1 + i)z - \sqrt{2}}$$

These generate the symmetries of the cube, which is a group isomorphic to  $A_4$ . Since  $f$  is invariant under the action of this group, it must factor through the quotient

$$f : \mathbb{P}^1 \longrightarrow \mathbb{P}^1/A_4 \longrightarrow \mathbb{P}^1$$

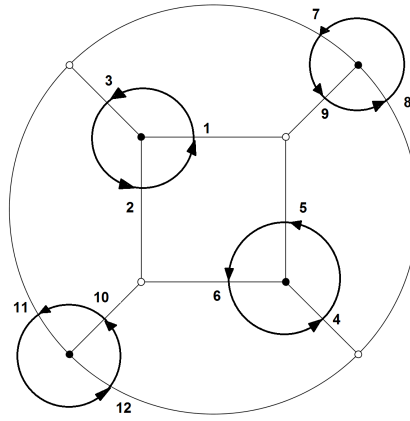
However, since the first arrow has degree 12, and  $f$  has degree 12, the second arrow must have degree 1, i.e. it must be an isomorphism of  $\mathbb{P}^1$  with itself. So  $f$  is the map we are looking for.

Given a Belyi map, the graph embedded in the surface is given by the preimage of  $[0, 1]$ , with the preimage of 0 as black points and the preimage of 1 as white points. In this particular case, we can plot the preimage of  $[0, 1]$ , to obtain the graph shown in Figure 1.4.

Figure 1.4: The preimage of  $[0, 1]$  by the map  $f$ .

The field extension we are looking at is the homomorphism of  $\mathbb{C}(t)$  into itself given by substitution of the variable by  $f$ . Thus, the extension is  $\mathbb{C}(f) \subset \mathbb{C}(z)$ .

We can also look at the monodromy. We want to know the action of the loops  $x$  and  $y$  which we described earlier on a fiber of the map. We can take any point in the interior of  $[0, 1]$ . For instance,  $1/2$ . Now, for a point in the preimage of  $1/2$ , that is, a point in one of the edges of the dessin, lifting the loop around 0 is just turning counterclockwise around the black vertex incident to that edge until we meet another edge.

Figure 1.5: The 12 liftings of the path  $x$  to the cube.

Thus, every edge is mapped to another edge, and we get a permutation of 12 elements. We can do the same with the loop around 1. In this case, the map we obtain is

$$x \mapsto (1, 3, 2)(4, 5, 6)(7, 9, 8)(10, 11, 12)$$

$$y \mapsto (1, 5, 9)(2, 10, 6)(3, 7, 11)(4, 12, 8)$$

And also, the subgroup of  $F_2$  which is the stabilizer of a point has index 12, since this is the size of the orbit (recall that these are equal!), so it is the preimage of the identity. Therefore, it is the normal subgroup generated by

$$\{x^3, y^3, (xy)^2\}$$

Since these are relations that give  $A_4$  with these generators.

Using the cube as an example, we have seen something important: we can know the monodromy action by just looking at the picture! This will turn out to be very useful for us.

## 1.5 Regular dessins

The cube dessin was an example of a regular dessin. A regular dessin corresponds with many familiar concepts: a regular (or normal) cover, a normal subgroup, a proper action and a Galois extension. We will prove that all these notions coincide in a dessin d'enfant when we look at it from the various points of view.

**Definition 1.5.1.** An **automorphism** of a dessin is an invertible morphism from the dessin to itself.

No surprises here. Recall what we mean by a morphism in the different contexts: if we have a Belyi pair  $(C, f)$ , it is a map  $\varphi : C \rightarrow C$  such that  $f \circ \varphi = f$ ; if we have a field extension, it is a morphism of extensions, i.e., a homomorphism  $\varphi : \mathbb{C}(C) \rightarrow \mathbb{C}(C)$  such that  $\varphi|_{\mathbb{C}(t)} = \text{id}$ , and if we have an action, it is a map commuting with the group action. In any of the formulations, it is clear that any morphism from a dessin to itself is invertible, and it is therefore an automorphism. Also, we can speak of the automorphism group in any of these settings, since we have seen that they are all equivalent.

**Proposition 1.5.2.** *Let  $(C, f)$  be a Belyi pair, let  $\mathbb{C}(t) \subset \mathbb{C}(C)$  be the corresponding field extension, and let  $F_2 \rightarrow X$  be the corresponding monodromy action. Let  $H$  be the subgroup of  $F_2$  associated with the action. The following are equivalent:*

1. *The order of the automorphism group of the dessin is equal to its degree.*
2.  *$(C, f)$  is a regular cover. That is, there exists a subgroup  $G < \text{Aut}(C)$  such that the map is equivalent to  $C \rightarrow C/G$ .*
3. *The extension  $\mathbb{C}(C)/\mathbb{C}(t)$  is a Galois extension.*
4.  *$H$  is a normal subgroup of  $F_2$ .*
5. *The action on  $X$  of the cartographic group is proper, i.e. if for any  $x \in X$  and  $g \in F_2$ , we have that  $x^g = x$ , then  $g = 1$ .*
6. *The order of the cartographic group is equal to the degree of the dessin.*

When any of these is true, we say that the dessin is a **regular dessin**.

*Proof.*

- 1  $\Leftrightarrow$  2) We have seen the idea for this when we talked about the cube. Let  $G$  be the automorphism group of the cover.  $G$  is a finite group, since its elements are determined by the image of an unramified point (therefore, its order is at most the degree of the dessin). Since  $G$  is a finite group, its action is properly discontinuous, and the quotient by it is a holomorphic map to another Riemann surface<sup>1</sup>.  $f$  must factor through this map, so there is a map  $\bar{f}$  which fits in the diagram

$$\begin{array}{ccc} C & \xrightarrow{f} & \mathbb{P}^1 \\ \downarrow \pi & \nearrow \bar{f} & \\ C/G & & \end{array}$$

Now we look at the degrees of the maps:  $G$  acts properly on the points on which  $f$  is not ramified, since an automorphism that fixes one of them must be the identity. Therefore, the degree of  $\pi$  equals  $|G|$ . However, we are assuming that  $|G|$  is also the degree of  $f$ , so the degree of  $\bar{f}$  must be 1. That is,  $\bar{f}$  is an isomorphism and  $\pi$  is equivalent to  $f$ .

Reciprocally, if the map is  $C \rightarrow C/G$ , then the group  $G$  is the group of automorphisms of the cover, since it obviously preserves the map, and therefore its order is at least the order of the fibers, which is the degree of the dessin. We have just seen that the order of the automorphism group is never bigger than the order of the fibers, so we are done.

- 2  $\Leftrightarrow$  3) Suppose that the Belyi map is  $C \rightarrow C/G$ , for some automorphism group  $G$ .  $\mathbb{C}(C/G)$  is a subfield of  $\mathbb{C}(C)$ , since  $\pi^*$  (with  $\pi$  as in the previous part) is a field homomorphism from  $\mathbb{C}(C/G)$  to  $\mathbb{C}(C)$ . The functions which are defined on  $C/G$  are the functions on  $C$  that factor through the quotient, i.e. the ones that  $G$  preserves. Thus, if we take  $G^* = \{\varphi^* : \varphi \in G\}$ , which is a subgroup of the Galois group  $\text{Gal}(\mathbb{C}(C)/\mathbb{C}(t))$ , the field  $\mathbb{C}(C/G)$  is the fixed field of  $G^*$ . The premise is that  $\pi : C \rightarrow C/G$  is the Belyi map, or in other words,  $\pi^* : \mathbb{C}(C/G) \rightarrow \mathbb{C}(C)$  is the inclusion of  $\mathbb{C}(t)$ , so  $\mathbb{C}(C/G) = \mathbb{C}(t)$ . This means that the fixed field of  $G^*$  is  $\mathbb{C}(t)$ , which in turn is the definition that the extension is Galois, and  $G^*$  must be the whole Galois group.

Now, suppose the extension  $\mathbb{C}(C)/\mathbb{C}(t)$  is Galois. Then, if we call  $G^* = \text{Gal}(\mathbb{C}(C)/\mathbb{C}(t))$ , we have that the fixed field of  $G^*$  is  $\mathbb{C}(t)$ . Every automorphism in  $G^*$  corresponds to an automorphism of  $C$  which

<sup>1</sup>See, for instance, Proposition 2.21 in [7], which proves it for Fuchsian groups, but the same proof applies. Nonetheless, the proof is essentially removing the fixed points and applying Proposition ??



preserves  $t$ , or in other words, an automorphism of  $(C, f)$ . Therefore, if we call  $G < \text{Aut}(C)$  the group corresponding to this Galois group, we have, as we had in the previous paragraph, that  $\mathbb{C}(t) = \mathbb{C}(C/G)$ , so the map is equivalent to  $C \longrightarrow C/G$ .

1  $\Rightarrow$  4) We are going to prove that the automorphism group is isomorphic to  $N_G(H)/H$ .

Suppose we have an action of  $F_2$  on a set  $X$ , and an automorphism  $\varphi : X \longrightarrow X$ . Pick an element  $x_0 \in X$ , and let  $H$  be its stabilizer. First, we are going to prove that  $\varphi$  is determined by  $\varphi(x_0)$ : indeed, since the action is transitive, every other  $x \in X$  is  $x_0^g$  for some  $g \in F_2$ . Then, (recall that we have defined the monodromy action on the right)

$$\varphi(x) = \varphi(x_0^g) = \varphi(x_0)^g$$

If  $\varphi$  is an automorphism. Now, let  $h \in F_2$  be such that  $\varphi(x_0) = x_0^h$ . Then,  $\varphi$ , as we have seen, must be  $\varphi(x_0^g) = \varphi(x_0)^g = x_0^{hg}$ , for every  $g \in F_2$ . In particular, this must be well-defined: if  $g_1, g_2$  are such that  $x_0^{g_1} = x_0^{g_2}$ , we must have

$$x_0^{hg_1} = \varphi(x_0^{g_1}) = \varphi(x_0^{g_2}) = x_0^{hg_2} \iff x_0^{hg_2g_1^{-1}h^{-1}} = x_0 \iff hg_2g_1^{-1}h^{-1} \in H$$

Since  $x_0^{g_1} = x_0^{g_2}$  is equivalent to  $g_2g_1^{-1} \in H$ , what we are saying is precisely that

$$hHh^{-1} = H$$

In other words,  $h \in N_G(H)$ . Also,  $h$  induces the identity if and only if  $x_0^h = x_0$ , so the automorphism group is in correspondence  $N_G(H)/H$ . If its size is the degree of the dessin, which is the index of  $H$ , this means that  $N_G(H) = F_2$ , which is what we are trying to prove.

4  $\Rightarrow$  5) Let  $H$ , as before, be the stabilizer of  $x_0$ . Then, the stabilizer of  $x_0^g$  is  $g^{-1}Hg$ . If  $H \triangleleft F_2$ , all the stabilizers are the same, and the intersection of all of them is  $H$ . Then, the morphism  $\varphi : F_2 \longrightarrow \mathcal{C}$  that has the cartographic group as its image has  $H$  as its kernel, since it is the intersection of all the stabilizers. Therefore, a permutation stabilizes a point if and only if it is in the image of  $H^g$  for some  $g$ , so it's in the kernel of the action.

5  $\Rightarrow$  6) The order of the cartographic group is the product of the order of the orbit, which is the degree of the dessin, by the order of the stabilizer of a point, which is 1, by hypothesis (since an element that fixes a point fixes all of them). Therefore, the order of the cartographic group must be equal to the degree of the dessin.

6  $\Rightarrow$  1) We know that the cartographic group is  $F_2/\text{Core}_{F_2}(H)$ . If the order of this group is the degree of the dessin, which is  $[F_2 : H]$ , this means that  $H = \text{Core}_{F_2}(H)$ , or in other words,  $H$  is normal in  $F_2$ . We have seen in the proof of 1  $\Rightarrow$  4 that the automorphism group is isomorphic to  $N_{F_2}(H)/H$ . Then, it follows that its order is the degree of the dessin.

□

There is one important conclusion in this proof: if a dessin is given by a subgroup  $H$  of  $F_2$ , its automorphism group is the quotient  $N_{F_2}(H)/H$ . It acts on points of  $X$  on the left: if we let  $\varphi_{h_1}, \varphi_{h_2}$  be the automorphisms that map  $x_0$  to  $x_0^{h_1}$  and  $x_0^{h_2}$ , for some  $h_1, h_2 \in N_{F_2}(H)$ , then

$$\varphi_{h_1}(\varphi_{h_2}(x_0)) = \varphi_{h_1}(x_0^{h_2}) = \varphi_{h_1}(x_0)^{h_2} = x_0^{h_1h_2} = \varphi_{h_1h_2}(x_0)$$

This is why we say that the automorphism group is  $N_{F_2}(H)/H$ .

We are going to make an important remark about notation: when we go from the automorphism group of a dessin, which is a subgroup of  $F_2$  acting on  $H \setminus F_2$  **on the left**, to a Galois group, we take a contravariant functor. Thus, for two elements  $g_1, g_2 \in F_2$ , or in  $N_{F_2}(H)/H$ , we have that  $(g_1g_2)^*$ , that lies in some Galois group, equals

$$(g_1 \circ g_2)^* = g_2^* \circ g_1^*$$

For this reason, we are going to adopt the convention that Galois groups always act **on the right**. This means that if  $\sigma, \tau \in \text{Gal}(F/K)$ , the product  $\sigma\tau$  is defined to be  $\tau \circ \sigma$ . If  $f \in F$ , we will write  $\sigma$  acting on  $f$  as  $f^\sigma$ , so we have that

$$(f^\sigma)^\tau = f^{\sigma\tau}$$

There is another conclusion to be drawn from the previous theorem: it follows that for a regular dessin, the degree of the field extension is equal to the degree of the map. In fact, the following is true:

**Proposition 1.5.3.** *Let  $C$  be a curve, and let  $f \in \mathbb{C}(C)$ . Then, the degree of  $f$  equals  $[\mathbb{C}(C) : \mathbb{C}(f)]$ .*

The proof for this fact can be found in [7], in chapter 1. However, we will not use it. We will prove the weaker statement that this only applies to Belyi pairs, and it is the only version of this statement we will use. To do it, we can use the regular cover.

**Proposition 1.5.4.** *Let  $(C, f)$  be a Belyi pair, with corresponding group  $H < F_2$ . Then, the regular cover of  $(C, f)$  corresponds to the Galois closure of  $\mathbb{C}(C)/\mathbb{C}(f)$  and to the group  $\text{Core}_{F_2} H$ .*

*Proof.* The most important part of the proof is the fact that the Galois closure of an extension isn't ramified at any new points. Take  $\mathbb{C}(C')/\mathbb{C}(f)$  to be the Galois closure of  $\mathbb{C}(C)/\mathbb{C}(f)$ . Also, take the regular cover  $(\tilde{C}, \tilde{f})$ . We wish to see that  $\tilde{C} = C'$ . The field extension  $\mathbb{C}(\tilde{C})/\mathbb{C}(f)$  is Galois, so it must contain  $\mathbb{C}(C')$ . However, if the extension  $\mathbb{C}(C')/\mathbb{C}(f)$  was ramified at a point other than  $0, 1, \infty$ , the extension  $\mathbb{C}(\tilde{C})/\mathbb{C}(f)$  would be too, but this is not the case.

Therefore, the three objects exist and satisfy universal properties that correspond to each other. Take the Galois closure of  $\mathbb{C}(C)/\mathbb{C}(f)$ . It corresponds to a regular Belyi pair  $(\tilde{C}, \tilde{f})$ , by Proposition 1.5.2. If this Belyi pair wasn't minimal, the minimal belyi pair would correspond to a smaller Galois extension. Also, since covers correspond to subgroups of  $F_2$  and regular covers to normal subgroups, the maximal normal subgroup, which is  $\text{Core}_{F_2} H$ , must correspond to the minimal regular cover.  $\square$

**Proposition 1.5.5.** *Let  $(C, f)$  be a Belyi pair. The degree of  $f$  equals  $[\mathbb{C}(C) : \mathbb{C}(f)]$ .*

*Proof.* Take its regular closure  $(\tilde{C}, \tilde{f})$ , which we have just seen corresponds to the Galois closure of  $\mathbb{C}(C)/\mathbb{C}(f)$ . Now, by the Galois correspondence, take the subgroup  $H^* < \text{Gal}(\mathbb{C}(\tilde{C})/\mathbb{C}(f))$  such that its fixed field is  $\mathbb{C}(C)$ . In the proof of 1.5.2. we saw that the fixed field of  $H^*$  corresponded to  $\mathbb{C}(\tilde{C}/H)$ . Now,

$$[\mathbb{C}(C) : \mathbb{C}(f)] = \frac{[\mathbb{C}(\tilde{C}) : \mathbb{C}(f)]}{[\mathbb{C}(\tilde{C}) : \mathbb{C}(C)]} = \frac{[\mathbb{C}(\tilde{C}) : \mathbb{C}(f)]}{[\mathbb{C}(\tilde{C}) : \mathbb{C}(\tilde{C}/H)]}$$

Since it's a regular dessin,  $[\mathbb{C}(\tilde{C}) : \mathbb{C}(f)] = \deg \tilde{f}$ , and since the extension in the denominator is Galois, its degree is  $|H|$ , which is equal to the degree of the map  $C \rightarrow C/H$ . Therefore,

$$[\mathbb{C}(C) : \mathbb{C}(f)] = \frac{[\mathbb{C}(\tilde{C}) : \mathbb{C}(f)]}{[\mathbb{C}(\tilde{C}) : \mathbb{C}(C)]} = \frac{\deg(\tilde{C} \rightarrow \mathbb{P}^1)}{\deg(\tilde{C} \rightarrow C)} = \deg(C \rightarrow \mathbb{P}^1)$$

$\square$

We have artfully avoided the pain of proving Proposition 1.5.3 for general curves and maps.

## 1.6 The field $\mathcal{K}$

We are going to see dessins d'enfants, instead of as abstract extensions, as subextensions of one given extension  $\mathcal{K}/\mathbb{C}(t)$ , very much in the same way as we see coverings of a space as subcoverings of its regular cover. For this section, we will also ask the reader to keep in mind that  $\mathbb{C}$  plays no special role, and that it can be replaced by  $\mathbb{Q}$  when the moment comes.

We are going to construct the field that is the union of all the extensions of  $\mathbb{C}(t)$  unramified outside of  $\{0, 1, \infty\}$ . To do this, consider the set  $\mathcal{H} = \{H < F_2 : [F_2 : H] < \infty\}$ . As we know, we can make each of these subgroups correspond to a dessin d'enfant, in fact, a dessin d'enfant with a base point (since, recall from Proposition 1.3.2 and Corollary 1.3.4, dessins d'enfants with a base point are in bijective correspondence with subgroups of the fundamental group). Therefore, we can make each subgroup correspond with an extension of  $\mathbb{C}(t)$ , although some of them may be isomorphic. The set  $\mathcal{H}$  is also ordered, by inclusion. We actually know, by Proposition 1.3.3, that for every two subgroups such that  $H_1 \subset H_2$ , there exists a unique morphism between the corresponding dessins preserving the base points. We can then define the following partially ordered set  $\mathcal{H}^*$ : it has one extension of  $\mathbb{C}(t)$  for every subgroup  $H$  of  $F_2$ , which we will call  $\mathcal{K}^H/\mathbb{C}(t)$ , and, whenever  $H_1 < H_2$ , it has the corresponding morphism between extensions  $i_{H_2 H_1} : \mathcal{K}^{H_2} \rightarrow \mathcal{K}^{H_1}$  which, as we have just said, is unique.

The set  $\mathcal{H}^*$  with these morphisms is actually a small category, since the compositions of the homomorphisms corresponding to inclusions  $H_1 \subset H_2$  and  $H_2 \subset H_3$  is the homomorphism corresponding to the inclusion

$H_1 \subset H_3$ . It is also a direct system: for every two subgroups  $H_1$  and  $H_2$ , we can take the subgroup  $H_1 \cap H_2$ , and the morphisms  $i_{H_1 H_1 \cap H_2} : \mathcal{K}^{H_1} \rightarrow \mathcal{K}^{H_1 \cap H_2}$ .

Using these fields and homomorphisms, their union is well-defined. If one is familiar with the notion of a direct limit, then the union is just the direct limit of this direct system of fields, and direct limits of direct systems exists in the category of fields. We will nonetheless prove this explicitly.

**Proposition 1.6.1.** *There exists a field extension  $\mathcal{K}/\mathbb{C}(t)$  such that every extension corresponding to a dessin d'enfant is contained in it, and it is minimal in the sense that any other extension satisfying this property contains an extension isomorphic to  $\mathcal{K}/\mathbb{C}(t)$  as a subextension.*

*Proof.* Consider the direct system  $\mathcal{H}^*$ . We will prove that there is a field  $\mathcal{K}$ , with a morphism of extensions for each  $H$ ,  $i_H : \mathcal{K}^H \rightarrow \mathcal{K}$ , such that, for any two extensions  $\mathcal{K}^{H_1}, \mathcal{K}^{H_2}$  such that one is contained in the other, the following diagram is commutative:

$$\begin{array}{ccc} & & \mathcal{K} \\ & \nearrow i_{H_2} & \uparrow i_{H_1} \\ \mathcal{K}^{H_2} & \xrightarrow{i_{H_2 H_1}} & \mathcal{K}^{H_1} \end{array}$$

Also, we require  $\mathcal{K}$  to be the minimal field with this property (this is the definition of direct limit). The way to construct it is the following: consider

$$\mathcal{K} = \frac{\bigsqcup_{H < F_2} \mathcal{K}^H}{\sim}$$

Where  $\bigsqcup$  stands for the disjoint union. In this union, we are going to write  $x_H$  to express that  $x_H \in H$ .  $\sim$  is the relation given by:

$$x_{H_1} \sim y_{H_2} \iff i_{H_1 H_1 \cap H_2}(x_{H_1}) = i_{H_2 H_1 \cap H_2}(y_{H_2})$$

It is easy to check that this is an equivalence relation, using the fact that the fields form a directed set<sup>2</sup>. We will use square brackets to denote the equivalence classes for this relation. This quotient is a field, with the following operations:

$$\begin{aligned} [x_{H_1}] + [x_{H_2}] &= [i_{H_1 H_1 \cap H_2}(x_{H_1}) +_{\mathcal{K}^{H_1 \cap H_2}} i_{H_2 H_1 \cap H_2}(x_{H_2})] \\ [x_{H_1}] \cdot [x_{H_2}] &= [i_{H_1 H_1 \cap H_2}(x_{H_1}) \cdot_{\mathcal{K}^{H_1 \cap H_2}} i_{H_2 H_1 \cap H_2}(x_{H_2})] \end{aligned}$$

Where  $+_{\mathcal{K}^H}$  and  $\cdot_{\mathcal{K}^H}$  denote the sum and product in the given field. It is easy to check that  $\mathcal{K}$  is a field, it is just a lot of properties to check (starting with the fact that the operations are well defined).

From any field  $\mathcal{K}^H$  there is a homomorphism to  $\mathcal{K}$ , given by

$$x \mapsto i_H(x) = [x_H]$$

And it is actually a homomorphism of  $\mathbb{C}(t)$ -algebras. The fact that these homomorphisms commute with  $i_{H_2 H_1}$  is as easy to check, since

$$i_{H_1}(i_{H_2 H_1}(x)) = [i_{H_2 H_1}(x)_{H_1}] = [x_{H_2}] = i_{H_2}(x)$$

Where the middle equality comes just from the definition of the equivalence relation.

Suppose now that some other field  $\mathcal{K}'$  satisfied these properties with respect to the system  $\mathcal{H}^*$ : let  $i'_H : \mathcal{K}^H \rightarrow \mathcal{K}'$  be homomorphisms of extensions such that, for every  $H_1 \subset H_2$ ,  $i'_{H_2} = i'_{H_1} \circ i_{H_2 H_1}$ . Define  $i : \mathcal{K} \rightarrow \mathcal{K}'$  to be  $i([x_H]) = i'_H(x)$ . This is well defined thanks to the fact that the  $i'_H$  commute with the inclusions between fields, and also  $i \circ i_H = i'_H$ , which is the property we wanted. Thus,  $\mathcal{K}$  is the minimal field extension satisfying this property.

Now, if a field extension  $\mathcal{K}'/\mathbb{C}(t)$  contains every dessin d'enfant as a subextension, let us see that it must contain the system  $\mathcal{H}^*$ . First of all, such a field must contain every extension corresponding to a regular dessin. Since these are Galois extensions, there is only one copy of each, and let us call them  $\mathcal{K}^{H'}$ . We are going to prove that we can pick a base point (that is, a valuation), in every extension, in such a way that, whenever  $\mathcal{K}^{H'_1} \subset \mathcal{K}^{H'_2}$  (which will happen whenever  $H_2 \subset H_1$ , since these are Galois extensions, and there is only one isomorphic copy in each field), the restriction of the valuation in  $\mathcal{K}^{H'_2}$  to  $\mathcal{K}^{H'_1}$  is the base point of  $\mathcal{K}^{H'_1}$ . This is clear using induction: if we have defined the valuation in a finite extension  $F \subset \mathcal{K}'$ , we can extend it to another finite extension  $F' \supset F$ , and thus to every finite subextension of  $\mathcal{K}'$ . Since this process can always continue, we can take the valuation defined in the union of all these fields  $\mathcal{K}^{H'}$ , since they are a countable collection. Now, for every Galois extension, we can define  $i'_H : \mathcal{K}^H \rightarrow \mathcal{K}'$  so that its image is  $\mathcal{K}^{H'}$  and it maps the base point

<sup>2</sup>Constructing the direct limit when the objects are not fields requires modifications of this construction, but the one we are using works for this particular case with fields, and in which every morphism is injective.

to the base point (since there is a unique homomorphism that does this). It is clear, using that there is only one homomorphism that preserves base points, that we will have  $i'_{H_2} = i'_{H_1} \circ i_{H_2 H_1}$  as before, and that we can extend these maps  $i_H$  to extensions that are not Galois, since they are contained in Galois extensions, and we can obtain the maps  $i_H$  by restriction.  $\square$

We have constructed a field that contains all dessins d'enfants, since these correspond to all the subgroups  $H$ . Actually, every finite subextension of this field is a dessin d'enfant.

**Proposition 1.6.2.** *Let  $\mathcal{K}/K/\mathbb{C}(t)$  be a subextension of  $\mathcal{K}/\mathbb{C}(t)$  such that  $[K : \mathbb{C}(t)]$  is finite. Then, there is some  $H < F_2$  of finite order such that  $K = \mathcal{K}^H$ .*

*Proof.* Every element of  $\mathcal{K}$  belongs to some extension  $\mathcal{K}^H$ , and in particular it is algebraic over  $\mathbb{C}(t)$ . Then,  $K/\mathbb{C}(t)$  is an algebraic finite extension, so it is generated by one element  $f$ . This  $f$  lies in some  $\mathcal{K}^H$ , by the definition of  $\mathcal{K}$ . There exists one maximal  $H$  such that  $f$  lies in  $\mathcal{K}^H$ , since  $\mathcal{K}^H \cap \mathcal{K}^{H'} = \mathcal{K}^{HH'}$  (where  $HH'$  stands for the subgroup generated by  $H$  and  $H'$  in case they are not normal). If we pick this  $H$ , it must follow that  $\mathbb{C}(t)(f) = \mathcal{K}^H$ , since  $\mathbb{C}(t)(f)$  is a subextension of  $\mathcal{K}^H$ , but subextensions of the extension corresponding to a dessin correspond to subcovers. Therefore,  $\mathbb{C}(t)(f)/\mathbb{C}(t)$  corresponds to a dessin d'enfant, and therefore it equals  $\mathcal{K}^H$ , since this was the minimal one.  $\square$

We are interested in the Galois group  $\text{Gal}(\mathcal{K}/\mathbb{C}(t))$ . In order to talk about this group, we are going to stop for a bit to talk about Galois theory of infinite extensions. The reader familiar with the Galois correspondence in infinite extensions may skip the next section.

### 1.6.1 Galois theory of infinite extensions

Suppose we have an algebraic Galois extension  $E/K$ , that is, one such that the Galois group  $\text{Gal}(E/K)$  fixes only  $K$ . We intend to look at the relation between  $\text{Gal}(E/K)$  and  $\text{Gal}(F/K)$  when  $F$  ranges across the finite Galois subextensions of  $E/K$ .

First of all, the fields  $K$  which are finite Galois extensions of  $K$  form a direct system with the morphisms given by inclusion, and therefore, by the Galois correspondence, the Galois groups  $\text{Gal}(F/K)$  form an inverse system, by which we mean that, whenever  $F \subset F'$ , restriction gives an epimorphism

$$\pi_{F'F} : \text{Gal}(F'/K) \longrightarrow \text{Gal}(F/K)$$

And also, the composition of two restriction maps is another restriction. This system has an inverse limit. Let us define it just in case: if  $G$  is the limit of this system, it means that for every finite Galois subextension  $F$  there exists a homomorphism  $\pi_F : G \longrightarrow \text{Gal}(F/K)$ , such that whenever  $F \subset F'$ ,  $\pi_F = \pi_{F'F} \circ \pi_{F'}$ , and the group  $G$  is universal with respect to this property: if for another group  $H$ , there exist homomorphisms  $\rho_F : H \longrightarrow \text{Gal}(F/K)$  such that  $\rho_F = \pi_{F'F} \circ \rho_{F'}$ , then there is a unique homomorphism  $\rho : H \longrightarrow G$  such that  $\rho_F = \pi_F \circ \rho$  for every  $F$ .

We can write this in a diagram to make it easier to remember:

$$\begin{array}{ccc} & H & \\ \rho_F \swarrow & \downarrow \rho & \searrow \rho_{F'} \\ & \widehat{G} & \\ \pi_F \swarrow & & \searrow \pi_{F'} \\ \text{Gal}(F'/K) & \xrightarrow{\pi_{F'F}} & \text{Gal}(F/K) \end{array}$$

Note the analogy with our construction of the direct limit of fields (to obtain an equivalent diagram for direct limits of fields, one just needs to reverse all the arrows).

If we look at the Galois group  $\text{Gal}(E/K)$ , it certainly has homomorphisms  $\text{Gal}(E/K) \longrightarrow \text{Gal}(F/K)$ , since these are induced by restriction. This suggests that it might be isomorphic to this inverse limit.

Let us prove first that inverse limits of groups exist. The proof will yield an explicit way to see an inverse limit.

**Proposition 1.6.3.** *Let  $(\{G_i : i \in I\}, \{\varphi_{ij} : i, j \in I, i \leq j\})$  be an inverse system of groups, where  $I$  is a directed set,  $G_i$  are the groups and  $\varphi_{ij}$  denote the homomorphisms between them. Then, its inverse limit exists and it can be constructed as the subgroup of  $\prod_i G_i$  made of the elements  $(a_i)_I$  such that*

$$\pi_{ii'}(a_i) = a_{i'} \forall i \leq i'$$

*Proof.* The map from the direct limit to the groups is the projection on the coordinates, and the proof is analogous to the proof of Proposition 1.6.1, so we will leave it to the reader.  $\square$

We will denote inverse limits by  $\lim_{\leftarrow}$ .

**Proposition 1.6.4.** *Let  $E/K$  be an algebraic Galois extension. Then,*

$$\mathrm{Gal}(E/K) = \varprojlim_{F/K \text{ finite and Galois}} \mathrm{Gal}(F/K)$$

*Proof.* Take the map induced by the restrictions, from  $\mathrm{Gal}(E/K)$  to  $\prod \mathrm{Gal}(F/K)$ . The image of this map clearly lies inside the inverse limit, since the restriction to finite subextensions is compatible with the restrictions from one subextension to another. Also, it is injective: if  $\sigma \in \mathrm{Gal}(E/K)$  is mapped to the identity, then it acts as the identity on every finite subextension. Therefore, since any element belongs to some finite Galois extension, it is the identity on  $E$ . For surjectivity, one only needs to check that an automorphism for each finite subextension that commutes with restrictions obviously defines an automorphism of  $E/K$ .  $\square$

The groups that arise this way are called profinite.

**Definition 1.6.5.** A **profinite group** is a group that is an inverse limit of finite groups.

Clearly, Galois groups of algebraic extensions fall in this category. Profinite groups can be given additional structure, namely a topology.

**Definition 1.6.6.** Let  $E/K$  be an algebraic Galois extension. The **Krull topology** on  $\mathrm{Gal}(E/K)$  is the topology that has a basis consisting of the cosets of the groups  $\mathrm{Gal}(E/F)$ , where  $F$  ranges across all finite Galois extensions of  $F$ .

Equivalently, it is the weakest topology that makes all the restriction homomorphisms  $\mathrm{Gal}(E/K) \rightarrow \mathrm{Gal}(F/K)$  continuous, when the finite groups  $\mathrm{Gal}(F/K)$  are given the discrete topology.

It is clear that both definitions coincide: the preimages of points by a restriction homomorphism are open sets by definition, and also the cosets of any group of the form  $\mathrm{Gal}(E/F)$  are preimages of subsets of  $\mathrm{Gal}(E/\bar{F})$ , where  $\bar{F}$  is the Galois closure of  $F/K$ .

It is also clear that the definition makes the Galois group a topological group, since multiplication by a group element maps the basis to itself.

Also, if we have a map  $\pi_F : \mathrm{Gal}(E/K) \rightarrow \mathrm{Gal}(F/K)$  for each Galois extension  $F$ , then every map is continuous if and only if the corresponding map

$$\prod \pi_F : \mathrm{Gal}(E/K) \rightarrow \prod \mathrm{Gal}(F/K)$$

is continuous when the product on the right has the product topology. Since the latter map is inclusion, the Krull topology is the topology induced by the product topology<sup>3</sup>.

We can give nice characterizations of open and closed subgroups, which we will do now.

**Proposition 1.6.7.** *Let  $G = \lim_{\leftarrow} G_i$  be a profinite group. A subgroup  $H$  of  $G$  is open if and only if it is closed and of finite index.*

*Proof.* Let us see  $G$  as a subspace of the product  $\prod_i G_i$ . If  $H$  is open, it must contain some neighborhood of the identity, which is of the form  $\prod_i U_i$ , where  $U_i = G_i$  for all but finitely many of the  $i$ 's. Therefore the index of  $H$  is at most the product of the orders of the groups  $G_i$  for which  $U_i \subsetneq G_i$ , which is finite. Also, every coset of  $H$  is an open set, since  $G$  is a topological group, and the union of the ones different from  $H$  is open, and it is the complement of  $H$ , so  $H$  is closed.

Reciprocally, if  $H$  is closed and of finite index, its cosets are closed and the union of the ones different from  $H$  is the complement of  $H$  and a closed set.  $\square$

**Proposition 1.6.8.** *Let  $G$  be a profinite group as in the previous proposition. A subgroup  $H$  of  $G$  is closed if and only if it is an intersection of open subgroups.*

<sup>3</sup>Recall that the product topology on  $\prod X_i$  is the topology generated by sets of the form  $\prod U_i$ , where all the  $U_i$ 's are open sets of  $X_i$  and all but finitely many of them are equal to  $X_i$ .

*Proof.* The “if” part is clear: open subgroups are also closed, so their intersection is also closed.

Suppose now we have a closed subgroup  $H$ . We have the obvious inclusion

$$H \subset \bigcap_{U=\dot{U}, H < U} U$$

So what we have to prove is the reverse inclusion: that for every  $g \notin H$ , there is some open subgroup  $U$  containing  $H$  such that  $g \notin U$ . Let  $g \notin H$ . Since  $H$  is closed, there is a neighborhood of  $g$  that doesn't intersect  $H$ . As usual, it will be of the form  $V = \prod V_i$ , where almost all the  $V_i$ 's equal  $G_i$ . Let  $J$  be the set of indices for which  $V_i \neq G_i$ . We can assume that  $V_i = \{g_i\}$  when  $i \notin J$ , where  $g_i$  is the projection of  $g$  onto  $G_i$ . We can do this since this set will also be open and contained in the previous one.

Then, we can consider the open subgroup

$$U = G \cap \prod_{i \notin J} G_i \times \prod_{i \in J} \{1\}$$

It is the preimage of 1 in  $\prod_{i \in J} G_i$ , so if we take the minimum of  $J$ , and call it  $i_0$  (we are using that the set of indices is a directed set), this group is the same as

$$U = G \cap \prod_{i \neq i_0} G_i \times \{1_{G_{i_0}}\}$$

Look at the subgroup  $UH$ . It is open, since it is a union of cosets of the open group  $U$ , and it is indeed a subgroup, since  $U$  is normal. We claim that it doesn't contain  $g$ . If  $g \in UH$ , then  $V \cap H$  would be non-empty: There would have to be some element  $h \in H$  whose component in  $G_{i_0}$  were equal to  $g_{i_0}$ , and this element would belong to  $V$ .  $\square$

The Galois correspondence holds then the same as for finite Galois extensions, only one needs to replace subgroups of a finite Galois group by closed subgroups.

**Proposition 1.6.9.** *Open subgroups of  $\text{Gal}(E/K)$  are in correspondence with finite subextensions  $F/K$ , via the mutually inverse maps*

$$\begin{aligned} H < \text{Gal}(E/K) &\longmapsto E^H = \{a \in E : \sigma(a) = a \forall \sigma \in H\} \\ F/K &\longmapsto \text{Gal}(E/F) < \text{Gal}(E/K) \end{aligned}$$

*Proof.* Suppose we have a finite Galois subextension  $F/K$ . An element of  $\text{Gal}(E/K)$  belongs to  $\text{Gal}(E/F)$  if and only if it maps to the identity in  $\text{Gal}(F/K)$ , i.e. if it belongs to  $\prod_{F' \neq F} \text{Gal}(F'/K) \times \{1_{\text{Gal}(F/K)}\}$ . In particular,  $\text{Gal}(F/K) = \frac{\text{Gal}(E/K)}{\text{Gal}(E/F)}$ , and  $[F : K] = [\text{Gal}(E/K) : \text{Gal}(E/F)]$ .

Now, if  $F/K$  is not a Galois extension, we can take its Galois closure  $\bar{F}$  and do the same thing again. Then,  $\text{Gal}(E/F)$  will be the preimage of  $\text{Gal}(\bar{F}/F) < \text{Gal}(\bar{F}/K)$  by the projection. In particular, the identity involving the index holds, by the Galois correspondence for finite extensions.

Suppose now we have an open subgroup  $H$ . Then, it contains some neighborhood of the identity in  $\prod \text{Gal}(F/K)$ , of the form  $\prod U_K$ . Let  $\bar{K}$  be the Galois closure of the fields for which  $U_K \neq \text{Gal}(F/K)$ . It is a finite extension, and this neighborhood contains

$$\text{Gal}(E/K) \cap \prod_{F' \neq \bar{F}} \text{Gal}(F'/K) \times \{1_{\text{Gal}(\bar{F}/K)}\} = \text{Gal}(E/\bar{F})$$

Therefore, the fixed field of  $H$  is contained in  $\bar{F}$ , and  $H$  maps onto a subgroup of  $\text{Gal}(\bar{F}/K)$ .  $E^H$  is the fixed field of this subgroup and its degree over  $K$  is equal to  $[\text{Gal}(E/K) : H]$ , by the Galois correspondence for finite extensions.

The following are clear:

$$H < \text{Gal}(E/E^H); F \subset F^{\text{Gal}(E/F)}$$

But they must be equal, since both groups in the first case have the same index in  $\text{Gal}(E/K)$ , and both extensions have the same degree in the second case.  $\square$

**Proposition 1.6.10.** *Closed subgroups of  $\text{Gal}(E/K)$  are in correspondence with subextensions  $F/K$ , via the mutually inverse maps*

$$\begin{aligned} H < \text{Gal}(E/K) &\longmapsto E^H = \{a \in E : \sigma(a) = a \forall \sigma \in H\} \\ F/K &\longmapsto \text{Gal}(E/F) < \text{Gal}(E/K) \end{aligned}$$

*Proof.* Note that closed subgroups are the intersection of the open subgroups containing them, by proposition 1.6.8, and that subextensions are the union of the finite subextensions contained in them. For a set of extensions  $\{F_i/K\}$ , let us denote the field they generate by  $\langle \bigcup_i F_i \rangle$ . It is clear that, for a set of finite extensions  $\{F_i\}$ ,

$$\bigcap_i \text{Gal}(E/F_i) = \text{Gal}\left(E/\left\langle \bigcup_i F_i \right\rangle\right)$$

If some  $\sigma \in \text{Gal}(E/K)$  fixes every field  $F_i$ , it will fix the field they generate. Reciprocally, if it fixes the field they generate, it will fix each one.

Also, if we have some open subgroups  $\{H_i\}$ ,

$$\text{Gal}\left(E/\left\langle \bigcup_i E^{H_i} \right\rangle\right) = \bigcap_i \text{Gal}(E/E^{H_i}) = \bigcap_i H_i$$

Let us prove that  $\text{Gal}(E/E^{\bigcap_i H_i}) = \bigcap_i H_i$ . The inclusion  $\text{Gal}(E/E^{\bigcap_i H_i}) \supset \bigcap_i H_i$  is obvious. Now, take some element  $\sigma \in \text{Gal}(E/K) \setminus \bigcap_i H_i$ . There must exist some  $i_0$  such that  $\sigma \notin H_{i_0}$ , so  $\sigma$  won't fix  $E^{H_{i_0}} \subset E^{\bigcap_i H_i}$ . Therefore,  $\sigma \notin \text{Gal}(E/E^{\bigcap_i H_i})$ . Using this, we have that

$$\left\langle \bigcup_i E^{H_i} \right\rangle = E^{\text{Gal}(E/\langle \bigcup_i E^{H_i} \rangle)} = E^{\bigcap_i H_i}$$

Where the first equality comes from the fact that  $E/K$  is Galois. Using these equalities, we can prove that the maps in the Galois correspondence are mutually inverse. Let  $H$  be a closed subgroup of  $\text{Gal}(E/K)$ . It is then equal to the intersection of the open subgroups containing them,  $H_i$ . It follows that

$$\text{Gal}(E/E^H) = \text{Gal}(E/E^{\bigcap_i H_i}) = \bigcap_i H_i = H$$

Also, if we have some extension  $F/K$ , it is the union of the finite extensions  $F_i$  it contains. Therefore,

$$E^{\text{Gal}(E/\langle \bigcup_i F_i \rangle)} = E^{\bigcap_i \text{Gal}(E/F_i)} = \left\langle \bigcup_i E^{\text{Gal}(E/F_i)} \right\rangle = \left\langle \bigcup_i F_i \right\rangle = F$$

□

Thus we have the Galois correspondence for any algebraic extension. We are just going to add one remark, which is that, the same as for finite extensions, if  $F/K$  is a subextension and  $\sigma \in \text{Gal}(E/K)$ , then  $\text{Gal}(E/\sigma(F)) = \sigma \text{Gal}(E/F) \sigma^{-1}$ .

This theorem on Galois theory is explained in Brian Osserman's notes [17], and for more information on profinite groups, one can look in [18].

### 1.6.2 Back to $\mathcal{K}$

We are going to use the results in the previous section to prove that the Galois group of  $\mathcal{K}/\mathbb{C}(t)$  is the inverse limit of Galois groups of the finite Galois subextensions, which correspond to the finite quotients  $F_2/N$ . This inverse limit is called the profinite completion.

**Definition 1.6.11.** Let  $G$  be a group. The set of its finite quotients  $G/N$  with the projections amongst them form an inverse system, and the inverse limit of this system is a profinite group, which we denote  $\widehat{G}$ , and it is the **profinite completion** of  $G$ .

Since the inverse limit can be seen as embedded in a product, we can see its elements as sequences, whose elements belong to the quotients of  $G$ .

As an example, what is the profinite completion of  $\mathbb{Z}$ ? It is made up of sequences of the form

$$(a_2, a_3, a_4, \dots)$$

Where  $a_n \in \mathbb{Z}/n\mathbb{Z}$ , and, whenever  $m|n$ ,  $a_n \equiv a_m \pmod{m}$ . So it has elements like

$$(1_2, 1_3, 1_4, \dots)$$

But also many other elements, like

$$(0_2, 2_3, 0_4, 3_5, 2_6, 4_7, 0_8, 5_9, \dots)$$

That may never become constant. The profinite completion of a group is, in general, a much larger group (for example,  $\widehat{\mathbb{Z}}$  is uncountable<sup>4</sup>). The group  $\widehat{\mathbb{Z}}$  arises for example as the Galois group of  $\overline{\mathbb{F}_p}/\mathbb{F}_p$ .

Back to  $\mathcal{K}$ : we are going to see that  $\text{Gal}(\mathcal{K}/\mathbb{C}(t)) = \widehat{F}_2$ . We know that this Galois group is the inverse limit of the Galois groups of finite Galois subextensions. These Galois groups are the finite quotients of the form  $F_2/N$ , and also, let's see that the restriction maps are equal to the projections in  $F_2$ .

Suppose we have some finite index  $N \triangleleft F_2$ . In Proposition 1.5.2 we said that  $\text{Gal}(\mathcal{K}^N, \mathbb{C}(t))$  is (canonically equivalent to) the automorphism group of the dessin corresponding to  $H$ , and that this in turn is the group  $N_{F_2}(N)/N = F_2/N$ . Therefore, the maps  $\pi_N : \text{Gal}(\mathcal{K}, \mathbb{C}(t)) \rightarrow \text{Gal}(\mathcal{K}^N, \mathbb{C}(t))$  map onto  $F_2/N$ .

Let us now prove that, if  $N_2 < N_1$  and both are (finite index) normal subgroups of  $F_2$ ,

$$\overline{\pi}_{N_1} = \pi_{N_2 N_1} \circ \overline{\pi}_{N_2}$$

Where  $\pi_{N_1 N_2}$  is the canonical projection from  $F_2/N_2$  onto  $F_2/N_1$ , and  $\overline{\pi}_{N_i}$  is the projection from  $\text{Gal}(\mathcal{K}, \mathbb{C}(t))$  onto  $\text{Gal}(\mathcal{K}^{N_i}, \mathbb{C}(t))$ . Let's see this. Let  $(C_i, f_i)$  be the dessin corresponding to  $N_i$ , and let  $p : C_2 \rightarrow C_1$  be the cover between them, that is, the map that maps the base point to the base point and such that  $f_2 = f_1 \circ p$ . We are going to prove that the projection  $F_2/N_2 \rightarrow F_2/N_1$  corresponds to restricting maps. Indeed, let  $g \in F_2$ , and call  $g_i$  the unique automorphism of  $(C_i, f_i)$  that maps the base point  $x_i$  to  $x_i^g$ . Then,

$$p \circ g_2 = g_1 \circ p$$

Both are covering maps from  $C_2$  to  $C_1$ , and to prove that they are equal, we just have to see where the base point maps to, by the unique lifting property. Since the monodromy action commutes with the covering maps,

$$p(g_2(x_2)) = p(x_2^g) = p(x_2)^g = g_1(p(x_2))$$

If in the equality  $p \circ g_2 = g_1 \circ p$  we take the corresponding maps in function fields, what we get is

$$g_2^* \circ i = i \circ g_1^*$$

In other words,  $g_1^*$  is just the restriction of  $g_2^*$  to the smaller extension  $\mathcal{K}^{N_1}/\mathbb{C}(t)$ . Now, if we have some  $\sigma \in \text{Gal}(\mathcal{K}/\mathbb{C}(t))$ , we can find some  $g_2$  such that  $g_2^* = \pi_{N_2}(\sigma)$ . Then,  $g_1^* = \pi_{H_1 H_2}(g_2^*)$ , and the equality is just saying that

$$\pi_{N_2 N_1}(\overline{\pi}_{N_2}(\sigma)) = \pi_{N_1 N_2}(g_2^*) = g_1^* = g_2^* \circ i = \sigma|_{\mathcal{K}^{N_1}} = \overline{\pi}_{N_1}(\sigma)$$

So we have proven, what we wanted, that the maps  $\pi_N : \text{Gal}(\mathcal{K}/\mathbb{C}(t)) \rightarrow F_2/N$  given by restriction commute with the projections between these quotients. Therefore, we have proven that  $\text{Gal}(\mathcal{K}/\mathbb{C}(t)) = \widehat{F}_2$ .

We can now use the Galois correspondence in  $\mathcal{K}/\mathbb{C}(t)$  to map extensions, or dessins d'enfants, to open subgroups of  $\widehat{F}_2$ . Suppose we have some open subgroup  $U \triangleleft \widehat{F}_2$ . The fixed field of  $U$  is  $\mathcal{K}^H$ , for some  $H < F_2$ . If we take some finite index normal subgroup  $N$  contained in  $H$ , then  $U = \text{Gal}(\mathcal{K}/\mathcal{K}^H)$  equals the preimage by the restriction of  $\text{Gal}(\mathcal{K}^N/\mathcal{K}^H) = H/N$ . Also, this preimage does not depend on the choice of  $N$ . Therefore, we can use  $\widehat{H}$  to name open subgroups of  $\widehat{F}_2$ , since every open subgroup arises in this way (as the preimage of  $H/N$ , where  $H < F_2$  and  $N$  is any finite index normal subgroup of  $F_2$  contained in  $H$ ).

**Corollary 1.6.12.** *Dessins d'enfants with a base point are in correspondence with open subgroups of  $\widehat{F}_2$ .*

*An open subgroup  $\widehat{H}$  has fixed field  $\mathcal{K}^H$  (and hence the notation).*

$F_2$  is embedded in  $\widehat{F}_2$ , by means of the projections from  $F_2$  to its quotients. Therefore, we can consider the image of finite index subgroups  $H < F_2$ . We are going to see that their closure in the Krull topology is  $\widehat{H}$ . Take the map  $i : F_2 \rightarrow \widehat{F}_2$ , and consider  $i(H)$ . Since closed subgroups correspond to subextensions,  $\overline{i(H)} = \text{Gal}(\mathcal{K}/\mathcal{K}^{i(H)})$ . Now, the fixed field of  $i(H)$  is precisely  $\mathcal{K}^H$ , so its closure is  $\widehat{H}$ .

From now on, we will omit the hat from the groups  $\widehat{H}$  and call them  $H$ , since they are both strongly related, and it will be clear from the context whether we are talking about a subgroup of  $F_2$  or an open subgroup of  $\widehat{F}_2$ . Most of the time from now on, we will refer to subgroups of  $\widehat{F}_2$ .

Let us consider dessins d'enfants without a base point: they are in bijection with conjugacy classes of subgroups of  $F_2$ . Since two subgroups  $H_1$  and  $H_2$  are conjugate in  $F_2$  if and only if they are conjugate in  $F_2/\text{Core}_{F_2}(H_1 \cap H_2)$ , which is a finite quotient, they will be conjugate if and only if they are also conjugate in  $\widehat{F}_2$ . Also, it is immediate to check, as it is for finite extensions, that for some  $\sigma \in \text{Gal}$  and some field  $F \subset \overline{K}$ ,  $\text{Gal}(\mathcal{K}/F^\sigma) = \text{Gal}(\mathcal{K}/F)^\sigma$ . Therefore, we have the following.

**Corollary 1.6.13.** *Dessins d'enfants without a base point are in correspondence with open subgroups of  $\widehat{F}_2$ , up to conjugation.*

<sup>4</sup>There are no countably infinite profinite groups!



## Part 2

# The Galois action on dessins d'enfants and Belyi's theorem

### 2.1 The Galois action

We are going to see how the Galois group of a field can act on a curve. We are going to use it first for the Galois group of the complex numbers  $\text{Gal}(\mathbb{C}/\mathbb{Q})$ , but in the next section we will prove Belyi's theorem, that states that every dessin d'enfant is defined over  $\overline{\mathbb{Q}}$ , so we will look at  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . Throughout this section,  $K$  will be any algebraically closed field of characteristic 0.

Recall that we said in section 1.5 that Galois groups would always act on the right. For coherence, we are going to keep this convention for  $\text{Gal}(K/\mathbb{Q})$ , so the action of some  $\sigma \in \text{Gal}(K/\mathbb{Q})$  on an element  $a \in K$  is given by  $a^\sigma$ , and it follows that  $(a^\sigma)^\tau = a^{\sigma\tau}$ .

Suppose we have a curve  $C$  defined over  $K$ , with field of rational functions  $K(C)$ , and some  $\sigma \in \text{Gal}(K/\mathbb{Q})$ . We are first going to define the action on the field of functions. We define  $K(C)^\sigma$  to be the  $K$ -algebra given by  $K \otimes_{\sigma^{-1}} K(C)$ .

This tensor product, as usual, is generated by all the elements of the form  $\{k \otimes_{\sigma^{-1}} f : k \in K, f \in K(C)\}$ , but we have the relation

$$k \otimes_{\sigma^{-1}} f = 1 \otimes_{\sigma^{-1}} k^{\sigma^{-1}} f$$

Since we also have that  $1 \otimes_{\sigma^{-1}} f_1 + 1 \otimes_{\sigma^{-1}} f_2 = 1 \otimes_{\sigma^{-1}} (f_1 + f_2)$ , all the elements in the tensor product can be written in the form  $1 \otimes_{\sigma^{-1}} f$ .

In this tensor product, the product by elements of  $K$  is given by

$$k(1 \otimes_{\sigma^{-1}} f) = k \otimes_{\sigma^{-1}} f = 1 \otimes_{\sigma^{-1}} k^{\sigma^{-1}} f$$

In other words, if  $i$  stands for the embedding of  $K$  in  $K(C)$ , the embedding of  $K$  in  $K(C)^\sigma$  is  $i \circ \sigma^{-1}$ . Note that  $\sigma$  induces a field isomorphism, from  $K(C)$  to  $K(C)^\sigma$ , which we will also call  $\sigma$ , given by  $f^\sigma = 1 \otimes_{\sigma^{-1}} f$ . However, this field isomorphism might not be a  $K$ -algebra isomorphism: if  $k \in K$  and  $f \in K(C)$ , then  $(kf)^\sigma = 1 \otimes_{\sigma^{-1}} kf = k^\sigma \otimes_{\sigma^{-1}} f = k^\sigma f^\sigma$ .

Suppose  $K(C) = K[x](y_1, \dots, y_n)/(f_1, \dots, f_m)$ . We are going to prove that

$$K(C)^\sigma \cong K[x](y_1, \dots, y_n)/(f_1^\sigma, \dots, f_m^\sigma)$$

Here, if  $f = \sum a_n x^n$ , then we define  $f^\sigma = \sum a_n^\sigma x^n$ . Also, the sign  $\cong$  stands for an isomorphism of  $K$ -algebras. We will prove it in the case where  $K(C) = K[x](y)/(f)$ , since the proof is the same, but the notation is clearer. If we call  $x^\sigma = 1 \otimes_{\sigma^{-1}} x$ , and  $y^\sigma = 1 \otimes_{\sigma^{-1}} y$ ,

$$f^\sigma(x^\sigma, y^\sigma) = \sum_{m,n} a_{mn}^\sigma (1 \otimes_{\sigma^{-1}} x)^m (1 \otimes_{\sigma^{-1}} y)^n = \sum_{m,n} a_{mn}^\sigma (1 \otimes_{\sigma^{-1}} x^m y^n) = \sum_{m,n} 1 \otimes_{\sigma^{-1}} a_{mn} x^m y^n = 0$$

Therefore,  $K(C)^\sigma \cong K[x](y)/(f^\sigma)$ . In particular,  $K(C)^\sigma$  has transcendence degree 1 over  $K$ .

This gives a right action of  $\text{Gal}(K/\mathbb{Q})$  on  $K$ -algebras, by which we mean that for two Galois elements  $\sigma, \tau \in \text{Gal}(K/\mathbb{Q})$ , there is a natural isomorphism of algebras between  $(K(C)^\sigma)^\tau$  and  $K(C)^{\sigma\tau}$ , given by

$$\begin{aligned} \cong: (K(C)^\sigma)^\tau &= K \otimes_{\tau^{-1}} K \otimes_{\sigma^{-1}} K(C) &\longrightarrow & K(C)^{\sigma\tau} = K \otimes_{\tau^{-1}\sigma^{-1}} K(C) \\ 1 \otimes_{\tau^{-1}} 1 \otimes_{\sigma^{-1}} a &\longmapsto & 1 \otimes_{\tau^{-1}\sigma^{-1}} a \end{aligned}$$

It is obviously a field isomorphism, and also, if  $k \in K$ ,

$$\begin{aligned} k(1 \otimes_{\tau^{-1}} 1 \otimes_{\sigma^{-1}} a) &= k \otimes_{\tau^{-1}} 1 \otimes_{\sigma^{-1}} a = 1 \otimes_{\tau^{-1}} k^{\tau^{-1}} \otimes_{\sigma^{-1}} a = \\ &= 1 \otimes_{\tau^{-1}} 1 \otimes_{\sigma^{-1}} k^{\tau^{-1}\sigma^{-1}} a \cong 1 \otimes_{\tau^{-1}\sigma^{-1}} k^{\tau^{-1}\sigma^{-1}} a = k(1 \otimes_{\tau^{-1}\sigma^{-1}} a) \end{aligned}$$

If we call  $\sigma$  the field isomorphism from  $K(C)$  to  $K(C)^\sigma$ , and we do the same for  $\tau$ , we get that  $\tau \circ \sigma = \sigma\tau$ , modulo this natural isomorphism. This means that for an element  $f \in K(C)$ ,

$$(f^\sigma)^\tau = 1 \otimes_{\tau^{-1}} 1 \otimes_{\sigma^{-1}} f \mapsto 1 \otimes_{\tau^{-1}\sigma^{-1}} f = f^{\sigma\tau}$$

In other words,  $(f^\sigma)^\tau = f^{\sigma\tau}$ , by means of this natural isomorphism.

**Definition 2.1.1.** Let  $C$  be a curve defined over  $K$ . For  $\sigma \in \text{Gal}(K/\mathbb{Q})$ , we define  $C^\sigma$  to be the curve that has  $K(C)^\sigma$  as its field of rational functions. Or, equivalently, if  $C = V(f_1, \dots, f_m)$ , then  $C^\sigma = V(f_1^\sigma, \dots, f_m^\sigma)$ .

This definition also gives a right action of  $\text{Gal}(K/\mathbb{Q})$  on the curves, since for two elements  $\sigma, \tau \in \text{Gal}(K/\mathbb{Q})$ , and a curve  $C$ ,

$$K((C^\sigma)^\tau) = K(C^\sigma)^\tau = (K(C)^\sigma)^\tau = K(C)^{\sigma\tau} = K(C^{\sigma\tau})$$

If a curve is transformed into another one by the action of the Galois group, we say that they are Galois conjugate.

The action of the Galois group is not trivial, and a curve can be Galois conjugate to a non-isomorphic one. As an example, take the plane curve given by the equation  $y^2 = x(x-1)(x-\sqrt{2})$ . It is Galois conjugate to the curve with equation  $y^2 = x(x-1)(x+\sqrt{2})$ , and these are not isomorphic (since the theory of elliptic curves says that the only curves isomorphic to  $y^2 = x(x-1)(x-\lambda)$  of the form  $y^2 = x(x-1)(x-\lambda')$  are the ones with  $\lambda' \in \left\{ \lambda, \frac{1}{\lambda}, 1-\lambda, 1-\frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda}{1-\lambda} \right\}$ ).

We want to define this action also on dessins d'enfants. In order to do this, we will first define the action on points and morphisms, which will allow us to see that the conjugate of a dessin is another dessin, and to find some invariants of the action.

We have a field isomorphism between  $K(C)$  and  $K(C)^\sigma$ , so we can use it to map valuations from one field to the other, and then use the correspondence between valuations and points. Take a valuation  $\nu$  of  $K(C)$ . This valuation is mapped to a valuation  $\nu^\sigma$  of  $K(C^\sigma)$ , by

$$\nu^\sigma(f^\sigma) = \nu(f)$$

This is the Galois action on the points of the curves. It is straightforward to check that this defines a  $K$ -valuation, using that  $\sigma$  is a field isomorphism. Note that, for two Galois automorphisms  $\sigma$  and  $\tau$ ,

$$(\nu^\sigma)^\tau((f^\sigma)^\tau) = \nu^\sigma(f^\sigma) = \nu(f) = \nu^{\sigma\tau}(f^{\sigma\tau}) = \nu^{\sigma\tau}((f^\sigma)^\tau)$$

Therefore,  $(\nu^\sigma)^\tau = \nu^{\sigma\tau}$ . Note that this definition is also  $\nu^\sigma = (\sigma^{-1})^*(\nu)$ .

If we have a morphism between two curves,  $\varphi : C \rightarrow C'$ , we can define  $\varphi^\sigma$  as well. We proceed like this: we take the morphism between the function fields  $\varphi^* : K(C) \rightarrow K(C')$ , and we define  $\varphi^{*\sigma} = \sigma \circ \varphi^* \circ \sigma^{-1}$ , that is,

$$\varphi^{*\sigma}(f^\sigma) = (\varphi^*(f))^\sigma$$

From the definition, it is clear both that  $(\varphi^{*\sigma})^\tau = \varphi^{*\sigma\tau}$ , and that the map  $\varphi^{*\sigma}$  is a  $K$ -algebra homomorphism.

We can now define the morphism  $\varphi^\sigma$  on points of  $C^\sigma$ , as  $(\varphi^{*\sigma})^*$ . Let us write this out explicitly: If we have a point in  $C$  corresponding to a valuation  $\nu$  of  $K(C)$  and a function  $f \in K(C')$ ,

$$(\varphi^\sigma(\nu^\sigma))(f^\sigma) = \nu^\sigma(\varphi^{*\sigma}(f^\sigma)) = \nu^\sigma((\varphi^*(f))^\sigma) = \nu(\varphi^*(f)) = (\varphi(\nu))(f)$$

Since  $(\varphi(\nu))^\sigma(f^\sigma) = (\varphi(\nu))(f)$ , it follows that

$$\varphi^\sigma(\nu^\sigma) = (\varphi(\nu))^\sigma$$

And, of course, the same thing happens if we change points for valuations.

So, if a point  $P$ , which corresponds to some valuation  $\nu$ , is mapped by  $\sigma$  to another point  $P^\sigma$ , with valuation  $\nu^\sigma$ , then

$$\varphi^\sigma(P^\sigma) = (\varphi(P))^\sigma$$

Of course, from the definition  $\varphi^\sigma = (\varphi^{*\sigma})^*$  follows that  $(\varphi^\sigma)^\tau = \varphi^{\sigma\tau}$ .

Suppose we have  $C = \mathbb{P}^1$ . Its field of functions is  $K(t)$ , and if we take an automorphism  $\sigma \in \text{Gal}(K/\mathbb{Q})$ , the field  $K(t)^\sigma$  is canonically isomorphic as a  $K$ -algebra to  $K(t)$ , by

$$\begin{aligned} \psi : K(t)^\sigma &\longrightarrow K(t) \\ 1 \otimes_{\sigma^{-1}} \frac{f(t)}{g(t)} &\longmapsto \frac{f^\sigma(t)}{g^\sigma(t)} \end{aligned}$$

It is straightforward to check that this is indeed a  $K$ -algebra isomorphism. We can then identify  $K(t)^\sigma$  with  $\psi(K(t)^\sigma) = K(t)$ , so that  $\psi \circ \sigma$  is just applying  $\sigma$  to the coefficients of functions (note that this action is the same as the one we have defined for polynomials). Since we can identify  $K(t)^\sigma$  with  $K(t)$  via this isomorphism, we can also identify  $\mathbb{P}^1$  with  $(\mathbb{P}^1)^\sigma$ . Now, let us see where the points are mapped. Suppose we have the point  $P$  with coordinates  $(1 : p)$ . This is the unique point where the function  $x_1/x_0 - p = t - p$  vanishes. By the identity

$$1 = \text{ord}_P(t - p) = \text{ord}_{P^\sigma}((t - p)^\sigma) = \text{ord}_{P^\sigma}(t - p^\sigma)$$

Where the last equality is the identification  $\psi$  we have just defined. Since  $t - p^\sigma$  has order 1 at  $P^\sigma$ , this must mean that the coordinates of  $P^\sigma$  are  $(1 : p^\sigma)$ . Thus,  $\sigma$  acts on  $\mathbb{P}^1$  by acting on the coordinates.

Now, suppose we have a curve  $C \subset \mathbb{P}^n$ , with coordinates  $(x_0 : \cdots : x_n)$ , and a point  $P = (p_0 : \cdots : p_n) \in C$ . Then,

$$\left(\frac{x_i}{x_j}\right)^\sigma(P^\sigma) = \left(\left(\frac{x_i}{x_j}\right)(P)\right)^\sigma = \left(\frac{p_i}{p_j}\right)^\sigma = \frac{p_i^\sigma}{p_j^\sigma}$$

Which means that  $\sigma$  acts on  $C$  by acting on the coordinates.

We could really just forget about the previous definitions and take the action on the coordinates as definition, but this way, we have clearly proven that the action doesn't depend on how a curve is embedded in  $\mathbb{P}^n$ .

Let us sum up all the definitions, the conclusions and the notation.

**Proposition 2.1.2** (The Galois action). *Suppose we have two curves  $C$  and  $C'$  defined over  $K$ , a point  $P \in C$ , a morphism  $\varphi : C \rightarrow C'$  and some  $\sigma \in \text{Gal}(K/\mathbb{Q})$ .*

- The field  $K(C)^\sigma$  is  $K \otimes_{\sigma^{-1}} K(C)$ .
- There is a field isomorphism  $\sigma : K(C) \rightarrow K(C)^\sigma$
- To a morphism of algebras  $\varphi^* : K(C) \rightarrow K(C')$  corresponds a morphism  $\varphi^{*\sigma} : K(C)^\sigma \rightarrow K(C')^\sigma$ , given by  $\varphi^{*\sigma}(f^\sigma) = (\varphi^*(f))^\sigma$ .
- The curve  $C^\sigma$  is such that  $K(C^\sigma) = K(C)^\sigma$ .
- The points of  $C^\sigma$  can be defined by  $\text{ord}_{P^\sigma}(f^\sigma) = \text{ord}_P(f)$ .
- To a morphism of curves  $\varphi : C \rightarrow C'$  corresponds a morphism  $\varphi^\sigma : C^\sigma \rightarrow C'^\sigma$  such that  $\varphi^\sigma(P^\sigma) = \varphi(P)^\sigma$ .
- $\varphi^{\sigma*} = \varphi^{*\sigma}$ .

We can now define the Galois action on dessins d'enfants. We see them as extensions  $K(f) \subset K(C)$ . The Galois action maps  $K(C)$  to another algebra  $K(C)^\sigma$ , and the subfield  $K(f)$  is mapped to some other subfield  $K(f)^\sigma$ , which is isomorphic to  $K(t)$  (it is the subfield generated by  $K^\sigma$  and  $f^\sigma$ ). The dessin d'enfant conjugate by  $\sigma$  to  $(C, f)$  is defined to be  $(C^\sigma, f^\sigma)$ , i.e. the extension  $K(f)^\sigma \subset K(C)^\sigma$ .

If the curve  $C$  is embedded, then we know the Galois action on the curve is given by applying  $\sigma$  to the coefficients of the equations. Also, since, for any function  $f = \frac{\sum a_\alpha \bar{x}^\alpha}{\sum b_\beta \bar{x}^\beta}$  (where  $\alpha$  and  $\beta$  are multiindices), and a point with coordinates  $\bar{p}$ ,

$$\frac{\sum a_\alpha (\bar{p}^\sigma)^\alpha}{\sum b_\beta (\bar{p}^\sigma)^\beta} = \left(\frac{\sum a_\alpha \bar{p}^\alpha}{\sum b_\beta \bar{p}^\beta}\right)^\sigma = f(P)^\sigma = f^\sigma(P^\sigma) = \frac{\sum c_\alpha (\bar{p}^\sigma)^\alpha}{\sum d_\beta (\bar{p}^\sigma)^\beta}$$

We must have that  $c_\alpha = a_\alpha^\sigma$  and  $d_\beta = b_\beta^\sigma$ , so applying  $\sigma$  to a function is applying  $\sigma$  to its coefficients.

Therefore, a definition for the Galois action on a Belyi pair can be just applying the automorphism to the coefficients of the equations of the curve and the Belyi function.

We must prove that the function  $f^\sigma$  is unramified outside of 0, 1 and  $\infty$ . Take a point  $P^\sigma \in C^\sigma$ . If  $f(P) = 0$ , then  $f^\sigma(P^\sigma) = 0^\sigma = 0$ , so the fiber of 0 is mapped to the fiber of 0. Also,  $\text{ord}_{P^\sigma} f^\sigma = \text{ord}_P f$ , so the ramification index is preserved. The same thing happens to the points over 1 and  $\infty$ . Also, if  $f^\sigma(P^\sigma) \notin \{0, 1, \infty\}$ , then  $f(P) \notin \{0, 1, \infty\}$ , so  $f$  is unramified at  $P$ . Therefore,

$$\text{ord}_{P^\sigma}(f^\sigma - f^\sigma(P^\sigma)) = \text{ord}_{P^\sigma}(f^\sigma - (f(P))^\sigma) = \text{ord}_P(f - f(P)) = 1$$

So the function  $f^\sigma$  is unramified over every point outside of  $\{0, 1, \infty\}$ . Therefore, it is a Belyi function.

If  $(C, f)$  is a Belyi pair, then  $\text{ord}_{P^\sigma} f^\sigma = \text{ord}_P f$ , so not only the ramification values are preserved, but also the set of ramification indices over each point. This is an example of a **Galois invariant**, a property of a dessin that is preserved under the Galois action. If we look at the bicolored graph, the index of ramification at a black or white point is the number of edges it has attached, and for a star vertex, it is half the number of edges on a face. Therefore, this means that a dessin d'enfant has the same number of points of each order and of faces of each number of sides as any of its Galois conjugates.

Since, by the Euler formula, the Euler characteristic is equal the number of vertices minus the number of edges plus the number of faces in any triangulation, this means that the genus of the underlying curve is another Galois invariant.

There is yet another invariant preserved by the Galois action, which is the automorphism group: the automorphism group of a dessin given by an extension  $K(C)/K(t)$  is  $\text{Gal}(K(C)/K(t))$ , and  $\sigma \in \text{Gal}(K/\mathbb{Q})$  acts on the homomorphisms in this Galois group. It is clear that the following map is an isomorphism:

$$\begin{aligned} \cdot^\sigma : \text{Gal}(K(C)/K(t)) &\longrightarrow \text{Gal}(K(C)^\sigma/K(t)) \\ \varphi &\longmapsto g^\sigma = \sigma \circ g \circ \sigma^{-1} \end{aligned}$$

Since its inverse is given by the corresponding map for  $\sigma^{-1}$ .

Also, a Galois automorphism  $\sigma$  will map Galois extensions of  $K(t)$  to Galois extensions (since they preserve the degree and the Galois group). It is clear then that it maps the Galois closure of an extension to the Galois closure of its image: in the language of Belyi covers, the Galois group preserves the regular cover of another cover. Now, since we know that the monodromy group of a dessin given by a finite index subgroup  $H$  of  $F_2$  (or an open subgroup of  $\widehat{F}_2$ ) is given by the quotient of  $F_2$  by the kernel of the action, which is  $\text{Core}_{F_2} H$ . Therefore, it is also the automorphism group of the regular dessin given by  $\text{Core}_{F_2} H$ , its regular cover. Since regular covers are preserved, their automorphism groups are also preserved, and these are the cartographic groups, we conclude that the cartographic group of a dessin is isomorphic to the cartographic group of a conjugate dessin. However, the dessins need not be isomorphic! This is because the Galois group doesn't necessarily map the canonical generators to the canonical generators, and the choice of these generators is what determines the dessin.

Let us sum up the Galois invariants so far:

**Proposition 2.1.3.** *The Galois action on dessins preserves the following:*

- *The degree of the covers.*
- *The ramification indices of points.*
- *The genus of the underlying curves.*
- *The automorphism group, up to isomorphism.*
- *The monodromy group, up to isomorphism.*

This action is what makes dessins d'enfants interesting, since it can be used to study the group  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  (since dessins d'enfants are defined over the algebraic field), for example by embedding it into other groups, as in proposition 2.3.1. This can be done because the action is faithful, i.e. for any  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , there is a dessin  $(C, f)$  that isn't fixed by  $\sigma$ . In fact, there is a dessin of a given genus [8] and also a regular dessin [9] such that they are not fixed by the action. For now, we will just prove that the action is not trivial.

**Proposition 2.1.4.** *Take the curve  $C$  with equation  $y^2 = x(x-1)(x-\sqrt{2})$ , and the function  $f(x, y) = x^2(2-x^2)$ . This function is a Belyi function, and if  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  is such that  $\sigma(\sqrt{2}) = -\sqrt{2}$ , then the Belyi pair  $(C^\sigma, f^\sigma)$  is not equivalent to  $(C, f)$ .*

*Proof.* It is straightforward to see that  $f$  is a Belyi function: its ramification points are  $\{(0, 0), (\sqrt{2}, 0), (1, 0), (-1, \pm\sqrt{-2-2\sqrt{2}}), (\sqrt{2}, 0), (0 : 1 : 0)\}$ , and their images are contained in  $\{0, 1, \infty\}$ .

The curve  $C^\sigma$  is not isomorphic to  $C$ , since this is the example we have seen before, so the dessins cannot be isomorphic. In fact, if we draw them, we obtain:



Figure 2.1: To the left, the dessin  $(C, f)$ , and to the right, the dessin  $(C^\sigma, f^\sigma)$ . Opposing edges of the rectangles are identified.

(Recall that an elliptic curve is a torus!). These drawings are clearly not isomorphic. For details on how to obtain the drawings, the reader can look at the method used in section 3.1 for a similar example.  $\square$

## 2.2 Belyi's theorem

This is the main theorem about dessins d'enfants.

**Theorem 2.2.1** (Belyi's Theorem). *Let  $C$  be a complex algebraic curve. The following are equivalent:*

1.  $C$  is defined over  $\overline{\mathbb{Q}}$ , i.e.  $C$  can be given by equations with coefficients in  $\overline{\mathbb{Q}}$ .
2.  $C$  has a Belyi map.

We will devote the rest of this section to proving Belyi's Theorem. We will follow closely the proof in [7].

### 2.2.1 Curves defined over the algebraic numbers have Belyi maps

Let's prove the first implication. Suppose we have a curve defined over  $\overline{\mathbb{Q}}$ . The process we are going to follow is: take a function on the curve  $f$ , look at its ramification values, and then compose it with functions  $g_i$  from  $\mathbb{P}^1$  to  $\mathbb{P}^1$  that will make the function  $g_k \circ g_{k-1} \circ \cdots \circ f$  have less and less ramification values, until we reach our objective, which is only three of them.

First of all, we will prove that we can make the ramification values rational.

**Lemma 2.2.2.** *Let a curve  $C \subset \mathbb{P}^n$  be given by equations  $f_1, \dots, f_m$ . Take coordinates  $(x_0 : \cdots : x_n)$ , and the affine part of the curve given by  $x_0 = 1$ . Fix a point  $P = (p_1, \dots, p_n) \in C$ , and consider the matrix  $Df = \left( \frac{\partial f_i}{\partial x_j} \Big|_P \right)_{ij}$ . Since the curve is non-singular, the matrix has rank  $n - 1$ .*

*A function of the form  $a_1x_1 + \cdots + a_nx_n$  will be ramified at  $P$  if and only if  $(a_1, \dots, a_n)$  lies in the span of the rows of  $Df$ .*

*Proof.* Taking a translation of affine space, we can assume that the point is the origin. Suppose  $(a_1, \dots, a_n) = (\lambda_1, \dots, \lambda_m)Df$ . Then, the polynomial  $f = \lambda_1 f_1 + \cdots + \lambda_m f_m$  is of the form  $a_1x_1 + \cdots + a_nx_n$  plus parts of degree greater than 1. Now, if  $\text{ord}_P(a_1x_1 + \cdots + a_nx_n) = 1$ , then  $\text{ord}_P(f)$  would be 1, since the rest of the terms in  $f$  have order at least 2. However,  $f$  is identically 0 on the curve, and therefore its order cannot be 1. So our function ramifies at  $P$ .

Now, take a function  $a_1x_1 + \cdots + a_nx_n$  that doesn't lie in the span of the rows of  $Df$ . This function along with the rows of  $Df$  span the whole space. Therefore, if this function were ramified, the curve wouldn't be non-singular, since a non-singular curve has an unramified function at every point.  $\square$

Therefore, if we have a curve that is defined over the algebraic numbers, we can take a coordinate function, and it will be ramified at the points where it lies in the span of  $Df$ . This can be expressed by saying that the ramified points are the points where some polynomials vanish, namely the minors of size  $n$  in the matrix made up of  $Df$  plus a row at the bottom for the coordinate function, plus the polynomials that define the function.

Therefore, the coordinates of the ramified points will be algebraic, i.e. the coordinate function will be ramified only over the algebraic numbers and  $\infty$ , since it might be ramified also at the points that don't lie in the affine part.

**Lemma 2.2.3.** *Let  $C$  be a curve defined over the algebraic numbers. Then, there is a map  $f \in \mathbb{C}(C)$  that ramifies only over values in  $\mathbb{Q} \cup \{\infty\}$ .*

*Proof.* Take a function  $f$ , as we have just done, that is ramified only over algebraic values. Let  $\{b_1, \dots, b_n\}$  be the ramification values of the function. Now, let  $g$  be the smallest degree polynomial in  $\mathbb{Q}[T]$  such that  $g(b_i) = 0$  for all the  $b_i$ 's, which means that  $P$  will be the product of the minimal polynomials of the  $b_i$ 's, removing repetitions.

Let us look at the function  $g \circ f$ . By the chain rule, for a point  $P$ ,  $\text{ord}_P(g \circ f) = \text{ord}_{f(P)}(g)e_P(f)$ , and therefore the ramification values of  $g \circ f$  are the ramification values of  $g$  plus the image by  $g$  of the ramification points of  $f$ . The latter set is contained in  $\{0, \infty\}$ , since we have constructed it this way. Let  $\{b'_1, \dots, b'_m\}$  be the ramification values of  $g$ , which are  $\{g(c_i) : g'(c_i) = 0\}$ . We can take their minimal polynomial again, call it  $g_1$ , and consider the function  $g_1 \circ g \circ f$ . We are going to see that the degree of  $g_1$  is strictly smaller than the degree of  $g$ .

Let  $g' = h_1^{\alpha_1} \cdots h_k^{\alpha_k}$  be the decomposition of  $g'$  into irreducible polynomials. The  $c_i$ 's are then the roots of these polynomials, in fact, we can number them  $c_1^1, \dots, c_{d_1}^1, c_1^2, \dots, c_{d_k}^k$ , so that  $c_j^i$  are the roots of  $h_i$ . Now, for a fixed  $i$ , the  $g(c_j^i) = b_j^i$ 's must be the roots of the same polynomial  $\tilde{h}_i$  of degree at most  $\deg h_i$ . Let us check this:  $\mathbb{Q}(g(c_j^i)) \subset \mathbb{Q}(c_j^i)$ , and the degree of the minimal polynomial is  $[\mathbb{Q}(g(c_j^i)) : \mathbb{Q}]$ , so  $\deg \tilde{h}_i \leq \deg h_i$ . Also, the minimal polynomial is the same for all of them, since we can take elements of the Galois group  $\sigma_j$ , such that  $c_j^i = (c_1^i)^{\sigma_j}$  (since they have the same minimal polynomial). Therefore, if  $\tilde{h}_i(c_1^i) = 0$ , then for every  $j$  we will have that  $\tilde{h}_i(c_j^i) = \tilde{h}_i((c_1^i)^{\sigma_j}) = (\tilde{h}_i(c_1^i))^{\sigma_j} = 0$ .

Therefore,  $g_2 = \tilde{h}_1 \cdots \tilde{h}_k$ , and  $\deg \tilde{h}_i \leq \deg h_i$ , so  $\deg g_2 \leq \deg g' < \deg g$ . We can iterate this process (take now the minimal polynomial of the ramification values of  $g_2$ ), and we will eventually reach a point where the degree is 0, and all the ramification points will be rational (there might be many of them, since we haven't kept track of  $g_1(0)$ , although we know it is rational, and the same for  $g_2(0)$ , and so on).  $\square$

We can now finish the proof of this part of the theorem.

**Lemma 2.2.4.** *Let  $\{q_1, \dots, q_m\} \subset \mathbb{Q}$ . There is a polynomial  $f$  that maps all these points to 0 and ramifies only over  $\{0, 1, \infty\}$ .*

*Proof.* We proceed by induction. If  $m = 2$ , then the polynomial  $-\frac{4}{(q_1 - q_2)^2}(x - q_1)(x - q_2)$  ramifies only at  $\frac{q_1 + q_2}{2}$  and its value there is 1, so we are done.

Suppose now that  $q_1 < q_2 < \dots < q_m$ . Take an affine transformation that maps  $q_1$  to 0 and  $q_3$  to 1. Let the image of  $q_2$  be  $\frac{m}{m+n}$ . If we take the polynomial  $P(x) = \frac{(m+n)^{m+n}}{m^m n^n} x^m (1-x)^n$ , one can check that its only ramification points are 0, 1,  $\frac{m}{m+n}$  and  $\infty$ . Their images are, respectively, 0, 0, 1,  $\infty$ , so the affine transformation composed with this polynomial maps  $\{q_1, \dots, q_m\}$  to a set of  $m - 1$  points, which contains its ramification values. We can iterate this process until we reach 2 points, and we are done.  $\square$

This ends the proof of the first part of Belyi's theorem. We have an easy corollary now: the Galois group acts faithfully on dessins.

**Proposition 2.2.5.** *The Galois group acts faithfully on dessins of genus 1.*

*Proof.* Recall from the classification of elliptic curves that every elliptic curve can be written in the form  $y^2 = x(x-1)(x-\lambda)$  for  $\lambda \in \mathbb{C} \setminus \{0, 1\}$ , and two such curves, for  $\lambda$  and  $\lambda'$ , are isomorphic if and only if  $\lambda' \in \left\{ \lambda, \frac{1}{\lambda}, 1-\lambda, 1-\frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda}{1-\lambda} \right\}$ , or, equivalently, if their  $j$ -invariants are equal, where

$$j(\lambda) = 256 \frac{(1 - \lambda(1 - \lambda))^3}{\lambda^2(1 - \lambda)^2}$$

Using this and Belyi's theorem, it is easy to produce dessins that change under the Galois action. Suppose we are given some  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \setminus \{\text{id}\}$ . Pick some  $j_0 \in \overline{\mathbb{Q}}$  such that  $\sigma(j_0) \neq j_0$ . Since  $j$  is surjective, there must be some  $\lambda \in \overline{\mathbb{Q}}$  such that  $j(\lambda) = j_0$  (and it will be different from 0 and 1).

Now, in virtue of Belyi's Theorem, we can pick a Belyi function  $f$  on the curve  $C$  with equation  $y^2 = x(x-1)(x-\lambda)$ . The conjugate Belyi pair will be defined on the curve  $C^\sigma$  with equation  $y^2 = x(x-1)(x-\lambda^\sigma)$ , which is not isomorphic to the first curve, since  $j(\lambda^\sigma) = (j(\lambda))^\sigma = j_0^\sigma \neq j_0$ . Therefore, the dessins must be non-isomorphic.  $\square$

### 2.2.2 Curves with Belyi functions are defined over $\overline{\mathbb{Q}}$

The key property we need to prove the reverse implication is the fact that curves with Belyi functions have finitely many Galois conjugates.

Suppose we have a Belyi pair  $(C, f)$ . The action of  $\text{Gal}(\mathbb{C}/\mathbb{Q})$  on it gives other Belyi pairs  $(C^\sigma, f^\sigma)$ , which have the same degree as the original one. The number of Belyi pairs of a given degree is finite, since the number of possible monodromy actions on a fixed number of points is clearly finite. Therefore, if a curve has a Belyi pair, it has finitely many distinct Galois conjugates.

It is in fact true that if a curve has finitely many conjugates, then it is defined over  $\overline{\mathbb{Q}}$ , that is, it can be given by equations with coefficients in  $\overline{\mathbb{Q}}$ . The proof can be found in chapter 3 of [7].

We are going to prove this in the special case of Belyi pairs. Now, in order to do this, we need to talk about specializations.

Suppose we have a finitely generated field  $K \subset \mathbb{C}$  over the rational numbers. We can pick a maximal transcendental set within  $K$ , which we can call  $\pi_1, \dots, \pi_n$ , and then, by the primitive element theorem, the extension will be of the form  $\mathbb{Q}(\pi_1, \dots, \pi_n, u)/\mathbb{Q}$ , where  $u$  is algebraic over  $\mathbb{Q}(\pi_1, \dots, \pi_n)$ . Let  $m_u$  be the minimal polynomial of  $u$  over  $\mathbb{Q}(\pi_1, \dots, \pi_n)$ . We can clear denominators in  $m_u$  so that  $m_u \in \mathbb{Q}[\pi_1, \dots, \pi_n][X]$ . If the resulting polynomial isn't monic, we can multiply  $u$  by some element of  $\mathbb{C}(\pi_1, \dots, \pi_n)$  to obtain a different  $u$  for which  $m_u$  is monic. From now on, we will assume that  $m_u$  is monic.

A **specialization** of  $(\pi_1, \dots, \pi_n)$  is just a set of complex numbers  $(\eta_1, \dots, \eta_n)$ . Note that, since the numbers are algebraically independent, there is a  $\mathbb{Q}$ -algebra homomorphism

$$s : \mathbb{Q}[\pi_1, \dots, \pi_n] \longrightarrow \mathbb{C}$$

Such that  $s(\pi_i) = \eta_i$ . Now, to extend this homomorphism to  $\mathbb{Q}[\pi_1, \dots, \pi_n, u]$ , it is needed that if we take the minimal polynomial  $m_u$  of  $u$ , and we apply  $s$  to its coefficients, to obtain a polynomial  $m_u^s$ , that  $m_u^s(s(u)) = 0$ .

In fact, this is sufficient: since  $\mathbb{Q}[\pi_1, \dots, \pi_n, u] \cong \mathbb{Q}[\pi_1, \dots, \pi_n][X]/(m_u)$ , a necessary and sufficient condition for a homomorphism from  $\mathbb{Q}[\pi_1, \dots, \pi_n, X]$  into  $\mathbb{C}$  to factor through this quotient is for the kernel to contain  $m_u$ .

Therefore, any specialization  $s$  of  $(\pi_1, \dots, \pi_n)$  gives some homomorphism into  $\mathbb{C}$  provided that we can find a root of  $m_u^s$ . To guarantee this, we choose the numbers  $\eta_i$  close to  $\pi_i$ .

We define the **distance** of a specialization  $(\eta_1, \dots, \eta_n)$  of  $(\pi_1, \dots, \pi_n)$  to be the maximum of  $|\pi_i - \eta_i|$  (recall that every number here is a complex number!).

**Lemma 2.2.6.** *Let  $(\pi_1, \dots, \pi_n; u)$  be complex numbers such that  $\pi_1, \dots, \pi_n$  are algebraically independent over  $\mathbb{Q}$  and  $u$  is algebraic over  $\mathbb{Q}(\pi_1, \dots, \pi_n)$ . Let  $m_u$  be the minimal polynomial of  $u$  over  $\mathbb{Q}[\pi_1, \dots, \pi_n]$ .*

*Let  $\delta > 0$  be a number such that it is smaller than  $|u_i - u_j|/2$ , where  $u_i, u_j$  are any distinct roots of  $m_u$ .*

*Then, there exists an  $\varepsilon$  such that for every specialization  $(\eta_1, \dots, \eta_n)$  of  $(\pi_1, \dots, \pi_n)$  of distance smaller than  $\varepsilon$ , the polynomial  $m_u^s$  has exactly one root  $u_s$  such that  $|u - u_s| < \delta$ .*

*Proof.* We just need to note that the coefficients of  $m_u$  are polynomials on  $\pi_i$ , and therefore continuous functions. Also, the roots of a polynomial depend continuously of its coefficients, so choosing close enough coefficients will yield roots of the polynomial  $m_u^s$  that are close enough to the roots of  $m_u$ .  $\square$

Specializations are the way we will change curves defined over transcendental fields by curves defined over  $\overline{\mathbb{Q}}$ , by using the fact that  $\overline{\mathbb{Q}}$  is dense in  $\mathbb{C}$ .

We want to prove that our curve  $C$  that has a Belyi function is isomorphic to another one whose coefficients are algebraic numbers. We are going to see how an isomorphism can be reduced to some polynomial equalities.

Take two Belyi pairs  $(C, f)$  and  $(C', f')$ . An isomorphism between them is equivalent, as we know, to an isomorphism of  $\mathbb{C}(t)$ -algebras

$$\Phi : \mathbb{C}(C) \longrightarrow \mathbb{C}(C')$$

By the primitive element theorem,  $\mathbb{C}(C)$  is generated over  $\mathbb{C}(t)$  by some  $x$ . Let  $F \in \mathbb{C}(t)[X]$  be its minimal polynomial. Then,

$$\mathbb{C}(C) \cong \frac{\mathbb{C}(t)[X]}{(F)}$$

And, analogously, there is some  $x'$  that generates  $\mathbb{C}(C')$  and some  $F' \in \mathbb{C}(t)[X]$  such that

$$\mathbb{C}(C') \cong \frac{\mathbb{C}(t)[X]}{(F')}$$

A  $\mathbb{C}(t)$ -algebra homomorphism from  $\mathbb{C}(C)$  to  $\mathbb{C}(C')$  is then determined by the image of  $x$ . The image of  $x$  will be some polynomial  $\Phi(x) = P_1(x')$ , where  $P_1 \in \mathbb{C}(t)$ . The map then takes  $P(x)$  to  $P(P_1(x'))$ , for any

$P \in \mathbb{C}(t)[X]$ . For the map to be well-defined, the necessary and sufficient condition is that  $F(x)$  maps to 0, that is, that  $F(P_1(X))$  equals 0 in  $\mathbb{C}(t)[X]/(F')$ . We can write this only in terms of polynomials, by saying that there exists  $H_1 \in \mathbb{C}(t)[X]$  such that

$$F(P_1(X)) = H_1(X)F'(X)$$

For an isomorphism, we need two mutually inverse morphisms, so there must be another morphism  $\Phi'$  given by another polynomial  $P_2$  so that  $x'$  will map to  $P_2(x)$ , and now there must exist a polynomial  $H_2$  such that

$$F'(P_2(X)) = H_2(X)F(X)$$

The final requirement is that the maps are mutually inverse. This means that  $\Phi'(\Phi(x)) = x$ . In other words, there exists some  $G_1 \in \mathbb{C}(t)[X]$  such that

$$P_1(P_2(X)) = X + G_1(X)F(X)$$

And also,  $\Phi \circ \Phi' = \text{id}$  is equivalent to there existing a polynomial  $G_2$  such that

$$P_2(P_1(X)) = X + G_2(X)F'(X)$$

These 4 equations are the way to express an isomorphism between covers, as we have just seen.

**Lemma 2.2.7.** *Let  $\mathbb{C}(C)/\mathbb{C}(t) \cong \mathbb{C}(t)[X]/(F)$  and  $\mathbb{C}(C)/\mathbb{C}(t) \cong \mathbb{C}(t)[X]/(F')$  be the extensions corresponding to two covers. There exists an isomorphism between both covers if and only if there exist  $P_1, P_2, H_1, H_2, G_1, G_2 \in \mathbb{C}(t)[X]$  such that the following identities hold:*

$$F(P_1(X)) = H_1(X)F'(X) \tag{2.1}$$

$$F'(P_2(X)) = H_2(X)F(X) \tag{2.2}$$

$$P_1(P_2(X)) = X + G_1(X)F(X) \tag{2.3}$$

$$P_2(P_1(X)) = X + G_2(X)F'(X) \tag{2.4}$$

Let us now prove Belyi's theorem. Suppose we are given a Belyi pair  $(C, f)$  with its corresponding extension  $\mathbb{C}(C)/\mathbb{C}(t) \cong \mathbb{C}(t)[X]/(F)$ . Let  $K = \mathbb{Q}(\pi_1, \dots, \pi_n, u)$  be the field generated by the coefficients of  $F$ , where  $\pi_1, \dots, \pi_n$  are algebraically independent and  $u$  is algebraic over the field generated by the rest of them. The Belyi pair has finitely many Galois conjugates. Therefore, there are many Galois automorphisms  $\sigma$  that fix the cover and map  $(\pi_1, \dots, \pi_n)$  to some complex numbers  $\pi_i^\sigma = \pi_{n+i}$  such that the set  $(\pi_1, \dots, \pi_{2n})$  is an algebraically independent set.

Since the cover is fixed by  $\sigma$ , there exists an isomorphism

$$\Phi : \mathbb{C}(C) \longrightarrow \mathbb{C}(C^\sigma) \cong \mathbb{C}(t)[X]/(F^\sigma)$$

By lemma 2.2.7, this means that there exist polynomials such that

$$F(P_1(X)) = H_1(X)F^\sigma(X)$$

$$F^\sigma(P_2(X)) = H_2(X)F(X)$$

$$P_1(P_2(X)) = X + G_1(X)F(X)$$

$$P_2(P_1(X)) = X + G_2(X)F^\sigma(X)$$

Take the field  $K_2$  generated by the coefficients of all of these polynomials. We can add some elements  $\pi_{2n+1}, \dots, \pi_d$  to our list  $\pi_1, \dots, \pi_{2n}$  so that they are a maximal algebraically independent set within  $K_2$ . Then, there exists some  $v$  such that  $K_2 = \mathbb{Q}(\pi_1, \dots, \pi_d, v)$ .

Now we are going to take a specialization of the above formulas, in order to define an isomorphism between  $\mathbb{C}(C)$  and some other curve defined over  $\overline{\mathbb{Q}}$ . We have seen in lemma 2.2.6 that there exists some  $\varepsilon$  such that every specialization of  $(\pi_1, \dots, \pi_d)$  of distance smaller than  $\varepsilon$  can be extended to a  $\mathbb{Q}$ -algebra homomorphism

$$s : \mathbb{Q}[\pi_1, \dots, \pi_d, v] \longrightarrow \mathbb{C}$$

Since  $\overline{\mathbb{Q}}$  is dense in  $\mathbb{C}$ , we can take a specialization with distance smaller than  $\varepsilon$  given by

$$(\eta_1 = \pi_1, \dots, \eta_n = \pi_n, q_{n+1}, \dots, q_d)$$



With  $q_i \in \overline{\mathbb{Q}}$ .

Now,  $s$  is a homomorphism of  $\mathbb{Q}$ -algebras, and it can of course be extended to  $\mathbb{Q}[\pi_1, \dots, \pi_d, v][t, X]$ , with image in  $\mathbb{C}[t, X]$ .

We want to extend  $s$  to the polynomials  $F^\sigma, H_1, H_2, G_1, G_2$ , and we can do this if we are careful: their coefficients, if we see them as rational functions in  $t$  and  $X$ , are elements of  $K_2$ , and thus rational functions in  $\pi_1, \dots, \pi_d, v$ , whose denominators might vanish in the specialization. However, the numbers  $(\eta_1 = \pi_1, \dots, \eta_n = \pi_n, q_{n+1}, \dots, q_d)$  that will make one of these denominators vanish will lie in some closed set of  $\mathbb{C}$ . Therefore, since we have a whole ball around each  $\pi_i$  to choose from, we can still pick elements that won't make these denominators vanish.

Also, if we see  $F^\sigma, H_1, H_2, G_1, G_2$  as polynomials in  $X$ , their coefficients are rational functions in  $\mathbb{C}(t)$ , whose denominators might also vanish. However, we can do the same thing, since the specializations that make this happen lie in a closed set of  $\mathbb{C}^d$ .

Therefore, there exists some distance  $\varepsilon$ , such that for any specialization of this distance, the image of the polynomials  $F^\sigma, H_1, H_2, G_1, G_2$  will be well-defined, since it will lie in the subring of

$$\mathbb{Q}(\pi_1, \dots, \pi_d, v, t, x)$$

In which  $s$  can be defined (rational functions whose denominators don't vanish). We can also take the specialization so that  $\pi_{n+1}, \dots, \pi_d$  are algebraic. Also,  $F^s$  will equal  $s$ , for  $u$  can only be mapped to one possible  $u$ , provided  $\varepsilon$  is small enough, so  $s(u) = u$ . Since  $s$  is a  $\mathbb{Q}$ -algebra homomorphism, and  $F^s = F$ , we will have that

$$\begin{aligned} F(P_1^s(X)) &= H_1^s(X)(F^\sigma)^s(X) \\ (F^\sigma)^s(P_2^s(X)) &= H_2^s(X)F(X) \\ P_1^s(P_2^s(X)) &= X + G_1^s(X)F(X) \\ P_2^s(P_1^s(X)) &= X + G_2^s(X)(F^\sigma)^s(X) \end{aligned}$$

In other words, if we use proposition 2.2.7, we obtain that the extension  $\mathbb{C}(C)/\mathbb{C}(t)$  is isomorphic to the extension  $\mathbb{C}(t)[X]/((F^\sigma)^s)$ , and the coefficients of  $(F^\sigma)^s$  are algebraic.

We can finally prove that we can define dessins over  $\overline{\mathbb{Q}}$  by using the fact that every function field over  $\overline{\mathbb{Q}}$ , which is algebraically closed, corresponds to a smooth projective curve (this can be proven, for example, using the Riemann-Roch Theorem, as in [15]).

Also, we can prove that if we have two dessins  $\overline{\mathbb{Q}}(C_1)/\overline{\mathbb{Q}}(t)$  and  $\overline{\mathbb{Q}}(C_2)/\overline{\mathbb{Q}}(t)$  such that, when their scalars are extended to  $\mathbb{C}$ , they give isomorphic dessins, then the initial dessins are also isomorphic. The way to do this is to prove, also using specialization, that morphisms between covers can also be defined over  $\overline{\mathbb{Q}}$ .

**Lemma 2.2.8.** *Suppose we have two extensions corresponding to dessins d'enfants defined over  $\overline{\mathbb{Q}}$ , which we will call  $\mathbb{C}(C_1) = \mathbb{C}(t, x_1) = \mathbb{C}(t)[X]/(F_1)$ , and  $\mathbb{C}(C_2) = \mathbb{C}(t, x_2) = \mathbb{C}(t)[X]/(F_2)$ , where  $F_1, F_2 \in \overline{\mathbb{Q}}(t)[X]$ . Every morphism from  $\mathbb{C}(C_1)$  to  $\mathbb{C}(C_2)$  can be defined over  $\overline{\mathbb{Q}}$ , that is, it maps  $x_1$  to  $P(x_2)$ , where  $P \in \overline{\mathbb{Q}}(t)[X]$ .*

*Proof.* We have seen that a morphism  $\Phi$  from  $\mathbb{C}(C_1)$  to  $\mathbb{C}(C_2)$  is equivalent to a polynomial  $P \in \mathbb{C}(t)[X]$ , such that  $\Phi(x_1) = P(X)$ , for which there exists another polynomial  $G \in \mathbb{C}(t)[X]$  such that

$$xF_1(P(X)) = G(X)F_2(X)$$

We are going to specialize this identity so that  $P \in \overline{\mathbb{Q}}(t)[X]$ . As usual, let  $(\pi_1, \dots, \pi_n, u)$  generate the field that contains the coefficients of all the polynomials involved. We can choose a specialization of small enough distance so that  $u$  is mapped by the  $\mathbb{Q}$ -algebra homomorphism to one unique root of the image of its minimal polynomial. Also, if the distance is small enough, as before, no denominators will become 0 in the coefficients of the polynomials, and also the coefficients of  $F_1$  and  $F_2$  will remain unchanged. If we apply the resulting homomorphism  $s$ , we are left with

$$F_1(P^s(X)) = G^s(X)F_2(X)$$

So  $P^s(x_2) = \Phi(x_1)$  will be a root of  $F_1$  in  $\mathbb{C}(C_2)$ . However, there are only finitely many such roots, (since  $\mathbb{C}(C_2)$  is a field). And if we make the distance of the specialization smaller,  $P^s(x_2)$  will lie in some neighborhood of  $P(x_2)^1$ , that is a root of  $F_1$ , that will contain no other roots of  $F_1$ . Therefore,  $P^s(x_2)$  will equal  $P(x_2)$ , and the morphism will be defined over the algebraic numbers.  $G$  will also be defined over the algebraic numbers, since it is  $F_1(P)/F_2$ .  $\square$

<sup>1</sup>Since  $P^s(x_2)$  can be given by a finite set of complex numbers (the coefficients in the rational functions in  $t$  that are the coefficients of  $P^s$ ), we can give these values the topology of  $\mathbb{C}^N$ . Anyway, it is clear that the function mapping the specialization to  $P^s(x_2)$  is continuous, and that finite sets in  $\mathbb{C}^N$  are closed.

Therefore, morphisms of the dessins d'enfants over  $\overline{\mathbb{Q}}$  correspond bijectively to morphisms of dessins d'enfants over  $\mathbb{C}$ . In particular, if we have two extensions  $\overline{\mathbb{Q}}(C_1)/\overline{\mathbb{Q}}(t)$  and  $\overline{\mathbb{Q}}(C_2)/\overline{\mathbb{Q}}(t)$  such that, when the scalars are extended to  $\mathbb{C}$ , they give the same dessin d'enfant, they must be isomorphic.

Also, we have our directed set of extensions of  $\overline{\mathbb{Q}}(t)$ , that enables us to construct the field  $\mathcal{K}$ , which is the extension that contains all the dessins d'enfants, just as in the complex case (like we did in section 1.6). Since morphisms between dessins are defined over  $\overline{\mathbb{Q}}$ , we have that taking  $\overline{\mathbb{Q}}$  as the base field doesn't change the Galois group of the extensions corresponding to dessins d'enfants. Therefore, since  $\text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t))$  is the limit of the Galois groups of Galois subextensions, we have that

$$\text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t)) \cong \varprojlim_{(C,t) \text{ Belyi pairs}} \text{Gal}(\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(t)) \cong \varprojlim_{(C,t) \text{ Belyi pairs}} \text{Gal}(\mathbb{C}(C)/\mathbb{C}(t)) = \widehat{F}_2$$

### 2.3 The action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\widehat{F}_2$

Now that we know that dessins are defined over  $\overline{\mathbb{Q}}$ , we can talk about the action of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  (recall section 2.1). Recall that, for every dessin  $\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(t)$ , and every  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , there is a conjugate dessin  $\overline{\mathbb{Q}}(C^\sigma)/\overline{\mathbb{Q}}(t)$ , and furthermore, the Galois group also acts on morphisms between dessins, and it does so in a functorial way: if we have two morphisms  $\varphi, \psi$ , then

$$(\varphi \circ \psi)^\sigma = \varphi^\sigma \circ \psi^\sigma$$

If these morphisms are automorphisms of an extension, then, it is clear that the Galois action will give an isomorphism from  $\text{Aut}(C, f)$  to  $\text{Aut}(C^\sigma, f^\sigma)$  (from now on, we will avoid calling these automorphism groups  $\text{Gal}(\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(t))$ , to avoid confusion with  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ).

Since the groups  $\text{Aut}(C, f)$  are quotients of  $\widehat{F}_2$ , it is interesting to consider whether we can define an action of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  not just on its quotients, but on the whole group  $\widehat{F}_2$  (this should have been easy to guess, given this section's title). Our objective now will be to prove this fact.

There is something more that we want from this section: if we look at the fields  $\mathbb{Q}(t) \subset \overline{\mathbb{Q}}(t) \subset \mathcal{K}$ , we see that the extension  $\overline{\mathbb{Q}}(t)/\mathbb{Q}(t)$  is clearly Galois (since it is basically the same as the extension  $\overline{\mathbb{Q}}/\mathbb{Q}$ ), and its Galois group clearly is isomorphic to  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . Therefore,

$$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \text{Gal}(\overline{\mathbb{Q}}(t)/\mathbb{Q}(t)) \cong \frac{\text{Gal}(\mathcal{K}/\mathbb{Q}(t))}{\text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t))} = \frac{\text{Gal}(\mathcal{K}/\mathbb{Q}(t))}{\widehat{F}_2}$$

In other words, we have the following exact sequence:

$$1 \longrightarrow \widehat{F}_2 \longrightarrow \text{Gal}(\mathcal{K}/\mathbb{Q}(t)) \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow 1$$

For every exact sequence  $1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$ , there is an induced map  $H \longrightarrow \text{Out}(N)$ . Recall that, for a group  $G$ ,  $\text{Inn}(G)$  is the set of automorphisms given by conjugation in the group, and  $\text{Out}(G) = \frac{\text{Aut}(G)}{\text{Inn}(G)}$ . Thus there is a map  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Out}(\widehat{F}_2)$ .

An element of  $\text{Out}(\widehat{F}_2)$  permutes the conjugacy classes of subgroups of  $\widehat{F}_2$ , since it is a well-defined automorphism up to conjugation. This permutation is actually the Galois action we have defined on dessins: Suppose we have some  $\widehat{\sigma} \in \text{Gal}(\mathcal{K}/\mathbb{Q}(t))$  such that its class modulo  $\widehat{F}_2$  is  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . A dessin  $\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(t)$  is mapped to  $\overline{\mathbb{Q}}(C)^{\widehat{\sigma}}/\overline{\mathbb{Q}}(t)$ . If  $\overline{\mathbb{Q}}(C) = \overline{\mathbb{Q}}(t, x) \cong \overline{\mathbb{Q}}(t)[X]/(F)$ , then  $F^\sigma(x^{\widehat{\sigma}}) = (F(x))^{\widehat{\sigma}} = 0$ , so its image,  $\overline{\mathbb{Q}}(t, x^{\widehat{\sigma}})$ , is isomorphic, as an extension, to  $\overline{\mathbb{Q}}(t)[X]/(F^\sigma)$ , which is the Galois action we have already defined. Therefore, the subgroup  $\widehat{\sigma}^{-1}H\widehat{\sigma} < \widehat{F}_2 < \text{Gal}(\mathcal{K}/\mathbb{Q}(t))$  is the subgroup  $H^\sigma$ , up to conjugation.

**Proposition 2.3.1.** *The homomorphism  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Out}(\widehat{F}_2)$  we have just defined is injective.*

*Proof.* Every  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  is mapped to an element different from the identity. If some element weren't, its image would be an inner automorphism of  $\widehat{F}_2$ , and in particular, it would leave every conjugacy class of subgroups unchanged. However, we have seen that the Galois group acts faithfully on dessins (proposition 2.2.5), so  $\sigma$  can't be mapped to the identity of  $\text{Out}(\widehat{F}_2)$ .  $\square$

We are going to prove now that we can find a homomorphism  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Aut}(\widehat{F}_2)$ , and that actually, the extension we wrote before is split, so

$$\text{Gal}(\mathcal{K}/\mathbb{Q}(t)) = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ltimes \widehat{F}_2$$

Here's some basic facts from split extensions: an extension  $N \longrightarrow G \xrightarrow{f} H$  is **split** if there exists a homomorphism  $s : H \longrightarrow G$  such that it is a section, i.e.  $f \circ s = \text{id}_H$ . This happens if and only if  $G$  is isomorphic to the semidirect product of  $N$  and  $H$ , where  $H$  is identified with its image in  $G$  by  $s$ .

**Theorem 2.3.2.** *The sequence*

$$1 \longrightarrow \widehat{F}_2 \longrightarrow \text{Gal}(\mathcal{K}/\mathbb{Q}(t)) \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow 1$$

*splits.*

*Proof.* Let's try to define the map to  $\text{Aut}(\widehat{F}_2)$  now. Take some  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . Clearly,  $\sigma$  gives an isomorphism between  $\text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t))$  and  $\text{Gal}(\mathcal{K}^\sigma/\overline{\mathbb{Q}}(t))$ . However, both extensions are isomorphic, so what we need is a canonical way to identify them, so that  $\sigma$  is an automorphism, and the resulting function  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \times \text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t)) \longrightarrow \text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t))$  is indeed an action.

The canonical way is given by using the base points in dessins. In  $\mathcal{K}$ , every subextension corresponds to a dessin with a base point. If we have some  $\mathcal{K}^H \subset \mathcal{K}$ , there is a base point in the corresponding curve  $C$ , which we will call  $P_H$ . We could call it  $P_C$ , but one curve can have different dessins defined on it, or the same one with different base points, so it is nicer to associate it with the subgroup.

Recall that we defined the inclusions between subfields of  $\mathcal{K}$  so that they would preserve the base point (since morphisms correspond to inclusions between subgroups of  $F_2$ , and there is an inclusion if and only if there is a covering preserving base points, see proposition 1.3.3), so, if  $i : \mathcal{K}^{H_1} \longrightarrow \mathcal{K}^{H_2}$  is one such inclusion, then  $i^*(P_{H_2}) = P_{H_1}$ . Also, this means that we can define a valuation  $\widehat{P}$  in  $\mathcal{K}$ , such that its restriction to each  $\mathcal{K}^H$  is  $P_H$ .

Take some open subgroup  $H < \widehat{F}_2$  and  $\mathcal{K}^H$ . If we consider the dessin given by  $(\mathcal{K}^H)^\sigma$ , with the base point  $(P_H)^\sigma$ , then there is one unique subfield of  $\mathcal{K}$  such that the extensions are isomorphic taking the base points into account. That is, there exists a unique extension, which we will call  $\mathcal{K}^{H^\sigma}$ , and a unique isomorphism  $\varphi_{\sigma,H} : (\mathcal{K}^H)^\sigma \longrightarrow \mathcal{K}^{H^\sigma}$  such that  $\varphi_{\sigma,H}^*(P_{H^\sigma}) = P_H^\sigma$ . When we have defined the action of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  on  $\widehat{F}_2$ , we will have that  $\overline{K}^{H^\sigma}$  is indeed the fixed field of  $H^\sigma$ , but for now consider it just as notation.

Thus we have, for each open subgroup  $H < \widehat{F}_2$ , an isomorphism (of extensions) from  $(\mathcal{K}^H)^\sigma$  to some  $\mathcal{K}^{H^\sigma}$ . We have to prove that this induces a morphism

$$\varphi_\sigma : \mathcal{K}^\sigma \longrightarrow \mathcal{K}$$

Let us check that it is. Suppose we have two open subgroups  $H_1 < H_2$ , and the corresponding homomorphism  $i_{H_2H_1} : \mathcal{K}^{H_2} \longrightarrow \mathcal{K}^{H_1}$ . Since  $\mathcal{K}^{H_i^\sigma}$  are isomorphic extensions to  $(\mathcal{K}^{H_i})^\sigma$ , and their base points are carried over by these isomorphisms, there will be a unique inclusion  $i_{H_2^\sigma H_1^\sigma}$  between them preserving the base point. What we need to check for  $\varphi_\sigma$  to be defined that the following diagram (of homomorphisms of  $\mathbb{C}(t)$ -algebras) is commutative:

$$\begin{array}{ccc} (\mathcal{K}^{H_1})^\sigma & \xrightarrow{\varphi_{\sigma,H_1}} & \mathcal{K}^{H_1^\sigma} \\ \uparrow i_{H_2H_1}^\sigma & & \uparrow i_{H_2^\sigma H_1^\sigma} \\ (\mathcal{K}^{H_2})^\sigma & \xrightarrow{\varphi_{\sigma,H_2}} & \mathcal{K}^{H_2^\sigma} \end{array}$$

It is indeed: there is at most one morphism from  $(\mathcal{K}^{H_2})^\sigma$  to  $\mathcal{K}^{H_1^\sigma}$  such that the restriction of the valuation corresponding to  $P_{H_1^\sigma}$  is  $P_{H_2^\sigma}^\sigma$ . However,

$$(\varphi_{\sigma,H_1} \circ i_{H_2H_1}^\sigma)^*(P_{H_1^\sigma}) = i_{H_2H_1}^{\sigma*}(\varphi_{\sigma,H_1}^*(P_{H_1^\sigma})) = i_{H_2H_1}^{\sigma*}(P_{H_1}^\sigma) = (i_{H_1H_2}^*(P_{H_1}))^\sigma = P_{H_2}^\sigma$$

And also,

$$(i_{H_2^\sigma H_1^\sigma} \circ \varphi_{\sigma,H_2})^*(P_{H_1^\sigma}) = \varphi_{\sigma,H_2}^*(i_{H_2^\sigma H_1^\sigma}^*(P_{H_1^\sigma})) = \varphi_{\sigma,H_2}^*(P_{H_2^\sigma}) = P_{H_2}^\sigma$$

So the diagram commutes.

Therefore, we have a morphism

$$\varphi_\sigma : \mathcal{K}^\sigma \longrightarrow \mathcal{K}$$

And, for each  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , there is some automorphism  $\tilde{\sigma} \in \text{Gal}(\mathcal{K}/\mathbb{Q}(t))$  (it doesn't fix  $\overline{\mathbb{Q}}(t)$ , because  $\sigma$  doesn't give homomorphisms of extensions of  $\overline{\mathbb{Q}}(t)$ ) defined by

$$\tilde{\sigma} = \varphi_\sigma \circ \sigma$$

What we want to prove now is that

$$\sim: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t))$$

is a group homomorphism. It is clearly a section of the quotient  $\text{Gal}(\mathcal{K}/\mathbb{Q}(t)) \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , since it maps extensions  $\mathcal{K}^H/\overline{\mathbb{Q}}(t)$  to extensions that are isomorphic to  $(\mathcal{K}^H)^\sigma/\overline{\mathbb{Q}}(t)$ , because  $\varphi_\sigma$  is an isomorphism of  $\overline{\mathbb{Q}}(t)$ -algebras.

Let  $\sigma, \tau \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . Let us prove the following: (recall that the Galois group acts **on the right**)

$$\widetilde{\tau\sigma} = \widetilde{\sigma \circ \tau} = \widetilde{\sigma} \circ \widetilde{\tau} = \widetilde{\tau}\widetilde{\sigma}$$

We only need to check this in finite extensions, since their union is  $\mathcal{K}$ . Let  $\mathcal{K}^H$  be one such extension. What we are trying to prove is

$$\varphi_{\tau\sigma} \circ \sigma \circ \tau = \varphi_\sigma \circ \sigma \circ \varphi_\tau \circ \tau$$

As we said, it suffices to prove this when restricted to  $\mathcal{K}^H$ .

Let us sketch what we are trying to prove:

$$\begin{array}{ccccc} \mathcal{K}^H & \xrightarrow{\tau} & (\mathcal{K}^H)^\tau & \xrightarrow{\sigma} & (\mathcal{K}^H)^{\tau\sigma} \xrightarrow{\varphi_{\tau\sigma}} \mathcal{K}^{H^{\tau\sigma}} \\ & & \downarrow \varphi_\tau & & \\ & & \mathcal{K}^{H^\tau} & \xrightarrow{\sigma} & (\mathcal{K}^{H^\tau})^\sigma \xrightarrow{\varphi_\sigma} \mathcal{K}^{(H^\tau)^\sigma} \end{array}$$

Recall that for any  $\overline{\mathbb{Q}}$ -algebra  $A$ ,  $(A^\tau)^\sigma = A^{\tau\sigma}$ , so  $\sigma((\mathcal{K}^H)^\tau)$  actually equals  $(\mathcal{K}^H)^{\tau\sigma}$ , and  $\varphi_{\tau\sigma}$  is defined on it. We need to prove that the objects at the far right of the diagram are the same, and that the diagram commutes when we see them as the same object.

First of all,  $\varphi_\tau$  is an isomorphism of  $\overline{\mathbb{Q}}(t)$ -algebras, and  $(\mathcal{K}^H)^\tau$  is isomorphic as a  $\overline{\mathbb{Q}}(t)$ -algebra to  $\mathcal{K}^{H^\tau}$ . Also,  $\varphi_\tau^*(P_{H^\tau}) = P_H^\tau$ .

Since both algebras are isomorphic, their images by  $\sigma$  also are isomorphic, and the isomorphism between them is actually  $\varphi_\sigma^\tau$ . Let us trace back the point  $P_H$ : we have that  $\sigma^*((P_H^\tau)^\sigma) = \sigma^*(P_H^{\tau\sigma}) = P_H^\tau$ , by definition, and, on the lower part of the diagram,  $\sigma^*(P_{H^\tau}^\sigma) = P_{H^\tau}$ . Also,

$$\varphi_\tau^{\sigma*}(P_{H^\tau}^\sigma) = \varphi_\tau^{*\sigma}(P_{H^\tau}^\sigma) = (\varphi_\tau(P_{H^\tau}))^\sigma = (P_H^\tau)^\sigma = P_H^{\tau\sigma}$$

So  $\varphi_\tau^\sigma$  is an isomorphism between the objects in the third column which carries one base point to the other.

We have that  $(\mathcal{K}^H)^{\tau\sigma}$  and  $(\mathcal{K}^{H^\tau})^\sigma$  are extensions isomorphic by an isomorphism carrying  $P_{H^\tau}^\sigma$  to  $P_H^{\tau\sigma}$ . Now, by definition of  $\varphi_\sigma$ ,

$$\varphi_\sigma^*(P_{(H^\tau)^\sigma}) = P_{H^\tau}^\sigma$$

Also, by definition of  $\varphi_{\tau\sigma}$ ,

$$\varphi_{\tau\sigma}^*(P_{H^{\tau\sigma}}) = P_H^{\tau\sigma}$$

The whole situation can be summed up in the following diagram, which states what the images of points are:

$$\begin{array}{ccccccc} P_H & \xleftarrow{\tau^*} & P_H^\tau & \xleftarrow{\sigma^*} & P_H^{\tau\sigma} & \xleftarrow{\varphi_{\tau\sigma}^*} & P_{H^{\tau\sigma}} \\ & & \uparrow \varphi_\tau^* & & \uparrow \varphi_\tau^{\sigma*} & & \\ & & P_{H^\tau} & \xleftarrow{\sigma^*} & P_{H^\tau}^\sigma & \xleftarrow{\varphi_\sigma^*} & P_{(H^\tau)^\sigma} \end{array}$$

We can see that  $\mathcal{K}^{H^{\tau\sigma}}$  and  $\mathcal{K}^{(H^\tau)^\sigma}$  are isomorphic (as extensions), by an isomorphism preserving their base points, namely

$$\varphi_\sigma \circ \varphi_\tau^\sigma \circ \varphi_{\tau\sigma}^{-1}$$

Therefore, they are equal, and  $H^{\tau\sigma} = (H^\tau)^\sigma$ . This gives an action of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  on the open subgroups of  $\widehat{F}_2$ , which is a lifting of the one we already have on their conjugacy classes.

We also have that the square

$$\begin{array}{ccc}
(\mathcal{K}^H)^\tau & \xrightarrow{\sigma} & (\mathcal{K}^H)^{\tau\sigma} \\
\downarrow \varphi_\tau & & \downarrow \varphi_\tau^\sigma \\
\mathcal{K}^{H^\tau} & \xrightarrow{\sigma} & (\mathcal{K}^{H^\tau})^\sigma
\end{array}$$

Commutes by definition.

Also, the diagram

$$\begin{array}{ccc}
(\mathcal{K}^H)^{\tau\sigma} & & \\
\downarrow \varphi_\tau^\sigma & \searrow \varphi_{\tau\sigma} & \\
(\mathcal{K}^{H^\tau})^\sigma & \xrightarrow{\varphi_\sigma} & \mathcal{K}^{H^{\tau\sigma}}
\end{array}$$

Commutes because all the morphisms involved are isomorphisms of  $\overline{\mathbb{Q}}(t)$ -algebras, and they preserve the base points (this is written two diagrams above).

So finally, we have proven that

$$\widetilde{\tau\sigma} = \widetilde{\tau}\widetilde{\sigma}$$

Which is what we wanted to prove.  $\square$

Now that we have the splitting that makes  $\text{Gal}(\mathcal{K}/\mathbb{Q}(t)) = \widehat{F}_2 \rtimes \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , the lifting to  $\text{Aut}(\widehat{F}_2)$  is just

$$\sigma \mapsto (g \mapsto g^\sigma = \widetilde{\sigma}^{-1}\tau\widetilde{\sigma})$$

If we take an open subgroup  $H < \widehat{F}_2$ , and we apply this automorphism to it, we get that

$$h \in H \iff h|_{\mathcal{K}^H} = \text{id} \iff \widetilde{\sigma}h\widetilde{\sigma}^{-1}|_{\widetilde{\sigma}(\mathcal{K}^H)} = \text{id}$$

Since  $\widetilde{\sigma}(\mathcal{K}^H) = \mathcal{K}^{H^\sigma}$ , it follows that the subgroup that fixes  $\mathcal{K}^{H^\sigma}$  is  $H^\sigma$ , which is the reason why we called it that way in the first place.

### 2.3.1 The field of moduli and fields of definition

We are going to describe two special fields related to a dessin. Take a Belyi pair  $(C, f)$ , such that the curve is  $V(g_1, \dots, g_m) \subset \mathbb{P}^n$ . Take the field generated by the coefficients of the  $g_i$ 's and  $f$ . These are all algebraic, so this field is a number field  $K$ . We call it field of definition.

**Definition 2.3.3.** A **field of definition** of a Belyi pair  $(C, f)$ , or a dessin d'enfant, is a number field  $K$  such that both the curve  $C$  and the Belyi function  $f$  can be defined with coefficients in  $K$ .

A dessin can have many fields of definition: first of all, if some  $K$  is a field of definition, every field containing it is also a field of definition. Nonetheless, it is not even true that there must exist a smallest field of definition.

**Definition 2.3.4.** Let  $(C, f)$  be a Belyi pair, with a corresponding extension  $\mathcal{K}^H/\overline{\mathbb{Q}}(t)$ . A **model** for  $(C, f)$  over a number field  $K$  is a set of equations  $g_1, \dots, g_m$  over  $K$  such that  $C \cong V(g_1, \dots, g_m)$  and such that in these coordinates,  $f$  has equations in  $K$ .

Suppose we are given a finite extension  $A/\mathbb{Q}(t)$  of  $\mathbb{Q}(t)$  contained in  $\mathcal{K}$ . Then, this extension can be split into two parts: if we consider  $\mathbb{Q}(t) \subset A \cap \overline{\mathbb{Q}}(t) \subset A$ , we see that  $A \cap \overline{\mathbb{Q}}(t)$  is  $K(t)$  for some number field  $K$ . The second part is an finite extension of  $K(t)$  that doesn't intersect  $\overline{\mathbb{Q}}(t)$ , so it is of the form

$$K(t, x) \cong K(t)[X]/(F)$$

Where  $F \in K(t)[X]$ . Now, if we take the field  $\overline{\mathbb{Q}}A$ , that is, the largest field containing both, we are going to see that we get the field

$$\overline{\mathbb{Q}}(t, x) \cong \overline{\mathbb{Q}}(t)[X]/(F)$$

The extensions  $\overline{\mathbb{Q}}(t, x)/\overline{\mathbb{Q}}(t)$  and  $K(t, x)/K(t)$  must have the same degree, for

$$[\overline{\mathbb{Q}}(t, x) : \overline{\mathbb{Q}}(t)] = [\text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t)) : \text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t, x))] = [\text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t)) : \text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t)) \cap \text{Gal}(\mathcal{K}/K(t, x))]$$

And by the second isomorphism theorem, this equals

$$\begin{aligned} [\overline{\mathbb{Q}}(t, x) : \overline{\mathbb{Q}}(t)] &= [\text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t))\text{Gal}(\mathcal{K}/K(t, x)) : \text{Gal}(\mathcal{K}/K(t, x))] = \\ &= [\text{Gal}(\mathcal{K}/K(t)) : \text{Gal}(\mathcal{K}/K(t, x))] = [K(t, x) : K(t)] \end{aligned}$$

Therefore, the polynomial  $F$  is also irreducible in  $\overline{\mathbb{Q}}(t)[X]$ , so it is also the minimal polynomial of  $x$  over  $\overline{\mathbb{Q}}(t)$ . Therefore, as we wanted,  $\overline{\mathbb{Q}}(t, x) \cong \overline{\mathbb{Q}}(t)[X]/(F)$ .

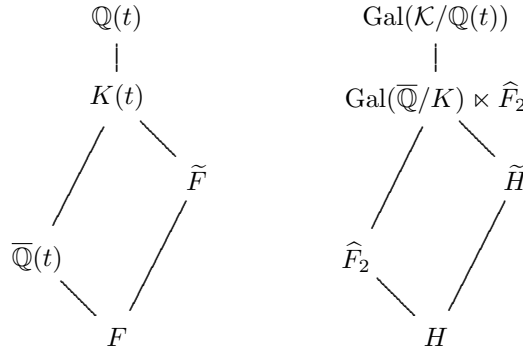
Suppose now that  $(C, f)$  is given by some equations defined over  $K$ , so that the extension is  $\overline{\mathbb{Q}}(t, x_1, \dots, x_n) \cong \overline{\mathbb{Q}}(t)[X_1, \dots, X_n]/(g_1, \dots, g_m)$ . We can consider the field  $K(t)[X_1, \dots, X_n]/(g_1, \dots, g_m)$ . For the same reasons as before, the intersection of this field with  $\overline{\mathbb{Q}}(t)$  will be  $K(t)$ , and the field generated by it and  $\overline{\mathbb{Q}}(t)$  will be the previous field. Therefore, we can see a model also as a field extension.

**Lemma 2.3.5.** *A model for a dessin given by an extension  $\mathcal{K}/F/\overline{\mathbb{Q}}(t)$  over a number field  $K$  is equivalent to a finite subextension  $\mathcal{K}/\tilde{F}/\overline{\mathbb{Q}}(t)$  such that  $\tilde{F} \cap \overline{\mathbb{Q}}(t) = K(t)$  and  $\overline{\mathbb{Q}}(t)\tilde{F} = F$ .*

Let us use the Galois correspondence to swap extensions for groups. Recall that  $\hat{F}_2$  is naturally included in  $\text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t))$ .

**Lemma 2.3.6.** *A model for a dessin given by an open subgroup  $H < \hat{F}_2$  is equivalent to an open subgroup  $\tilde{H}$  of  $\text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(t)) = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ltimes \hat{F}_2$  such that  $\tilde{F}_2\tilde{H} = \text{Gal}(\overline{\mathbb{Q}}/K) \ltimes \hat{F}_2$  and  $\tilde{H} \cap \hat{F}_2 = H$ .*

This comes from the equivalence of these diagrams:



Note that

$$\text{Gal}(\overline{\mathbb{Q}}/K) = \frac{\tilde{H}\hat{F}_2}{\hat{F}_2}$$

Is equivalent to the fact that the image of  $\tilde{H}$  by the projection onto  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  is  $\text{Gal}(\overline{\mathbb{Q}}/K)$ . Also, by the second isomorphism theorem,

$$\frac{\tilde{H}}{\tilde{H} \cap \hat{F}_2} \cong \frac{\tilde{H}\hat{F}_2}{\hat{F}_2} = \text{Gal}(\overline{\mathbb{Q}}/K)$$

Let us look now at another field related to a dessin: the field of moduli. Take a dessin, given by a subgroup  $H$ . Consider the subgroup  $\text{St}H < \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  made up of the automorphisms that fix the dessin (up to isomorphism, that is, to conjugation in  $\hat{F}_2$ ). If  $K$  is any field of definition of  $H$ , this subgroup obviously contains  $\text{Gal}(\overline{\mathbb{Q}}/K)$ . It is therefore a closed subgroup of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , and it has a fixed field defined by it. This field is called the field of moduli of the dessin.

**Definition 2.3.7.** The **field of moduli** of a dessin is the fixed field of the subgroup of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  that leaves it invariant.

If a dessin is given by a Belyi pair  $(C, f)$ , we denote it by  $\mathcal{M}(C, f)$ .

It is clear that any field of definition contains the field of moduli: If  $K$  is a field of definition, any element of  $\text{Gal}(\overline{\mathbb{Q}}/K)$  will fix the dessin, and therefore the subgroup that fixes the dessin contains  $\text{Gal}(\overline{\mathbb{Q}}/K)$ . Since inclusions are reversed by the Galois correspondence, the field of moduli is contained in any such  $K$ .

Suppose a dessin's field of moduli was indeed a field of definition. Then, it would be the minimal field of definition. Now, the question is: when is a dessin defined over its field of moduli? Actually, not every dessin is defined over its field of moduli. There is an example of this phenomenon in [4] and on section 2.5. Nonetheless, some dessins are defined over their field of moduli, such as regular dessins and dessins with no automorphisms. We will see this in short time.

Let us give an interpretation of the field of moduli in terms of subgroups of  $\text{Gal}(\mathcal{K}/\mathbb{Q}(t))$ , as we did with the field of definition.

As with any semidirect product, we can write the elements of  $\text{Gal}(\mathcal{K}/\mathbb{Q}(t)) = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ltimes \widehat{F}_2$  in a unique way as  $\tilde{\sigma}g$ , which we can write as  $(\sigma, g) \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \times \widehat{F}_2$  (we are not saying that the lifting of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  is unique, only that given this lifting, the way of writing the elements as pairs is unique), and the product is given by

$$(\sigma_1, g_1)(\sigma_2, g_2) = \tilde{\sigma}_1 g_1 \tilde{\sigma}_2 g_2 = \tilde{\sigma}_1 \tilde{\sigma}_2 \tilde{\sigma}_2^{-1} g_1 \tilde{\sigma}_2 g_2 = (\sigma_1 \sigma_2, g_1^{\sigma_2} g_2)$$

Now, suppose some  $\sigma$  fixes a dessin given by an open subgroup  $H$ . This means that  $H^\sigma = gHg^{-1}$  for some  $g \in \widehat{F}_2$ . If we see  $H$  as a subgroup of  $\text{Gal}(\mathcal{K}/\mathbb{Q}(t))$ , this means that, for every  $h \in H$ ,

$$(\sigma, g)^{-1}(1, h)(\sigma, g) = \left(\sigma^{-1}, (g^{-1})^{\sigma^{-1}}\right)(1, h)(\sigma, g) = (1, g^{-1}h^\sigma g) \in 1 \ltimes H$$

So we see that  $\sigma \in \text{St}H$  if and only if there is some  $g \in \widehat{F}_2$  such that  $(\sigma, g) \in N_{\text{Gal}(\mathcal{K}/\mathbb{Q}(t))}(H)$ .

To shorten the notation, we will call  $G = \text{Gal}(\mathcal{K}/\mathbb{Q}(t))$ .

Therefore, the field of moduli can be seen as the fixed field of the projection onto  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  of the group  $N_G(H)$ .

**Lemma 2.3.8.** *The field of moduli of a dessin corresponding to an open subgroup  $H < \widehat{F}_2$  is the projection onto  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  of  $N_G(H)$ .*

Take any model  $\tilde{H}$  for a dessin given by a subgroup  $H$ . Since  $\widehat{F}_2$  is normal in  $G$ , for any  $h \in \tilde{H}$ ,  $hHh^{-1} \subset \widehat{F}_2$ , but also, it is contained in  $\tilde{H}$ . Therefore,  $hHh^{-1} \subset \widehat{F}_2 \cap \tilde{H} = H$ , so  $\tilde{H} \subset N_G(H)$ .

If we have a dessin given by a Belyi pair  $(C, f)$  and a subgroup  $H$ , let us call  $\mathcal{M}(H) = \text{Gal}(\overline{\mathbb{Q}}/\mathcal{M}(C, f))$ . By the second isomorphism theorem,

$$\mathcal{M}(H) = \frac{N_G(H)}{N_G(H) \cap \widehat{F}_2} = \frac{N_G(H)}{N_{\widehat{F}_2}(H)} \cong \frac{N_G(H)\widehat{F}_2}{\widehat{F}_2}$$

**Proposition 2.3.9.** *A dessin given by a subgroup  $H$  is defined over its field of moduli if and only if the following exact sequence splits:*

$$1 \longrightarrow \frac{N_{\widehat{F}_2}(H)}{H} \longrightarrow \frac{N_G(H)}{H} \longrightarrow \mathcal{M}(H) \longrightarrow 1$$

*Proof.* Recall that a sequence  $1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$  splits if and only if there is a subgroup  $\tilde{H} < G$  such that  $\tilde{H} \cap N = 1$  and  $\tilde{H}N = G$ . A sketch of the proof goes as follows: if there is such a group, it maps bijectively onto the quotient  $H$ , so the inverse of this map is the desired section. Conversely, if there is a section, its image will be the subgroup  $\tilde{H}$ .

Therefore, we are saying that a field is defined over its field of moduli if and only if there is a subgroup  $\tilde{H} < N_G(H)/H$  such that

$$\tilde{H} \cap \frac{N_{\widehat{F}_2}(H)}{H} = 1; \tilde{H} \frac{N_{\widehat{F}_2}(H)}{H} = \frac{N_G(H)}{H}$$

If we call  $\tilde{H}$  the preimage of this group by the quotient by  $H$ , then  $\tilde{H} < N_G(\widehat{F}_2)$ , and

$$\tilde{H} \cap N_{\widehat{F}_2}(H) = H; \tilde{H}N_{\widehat{F}_2}(H) = N_G(H)$$

Therefore, if we look back to lemma 2.3.6, we have that  $\tilde{H}$  is a model for  $H$ . The field of definition of this model is the one with Galois group  $\tilde{H}/(\tilde{H} \cap \widehat{F}_2)$ . Since  $\tilde{H} < N_G(H)$ , then  $\tilde{H} \cap \widehat{F}_2 \subset N_{\widehat{F}_2}(H)$ , so  $\tilde{H} \cap \widehat{F}_2 = H$ , and therefore the Galois group of the model's field of definition is  $\tilde{H}/H \cong \mathcal{M}(H)$  (since  $\tilde{H}$  maps bijectively onto the fourth term in the exact sequence). In conclusion, if the sequence splits, there is a model defined over the field of moduli.

Reciprocally, if we have a model  $\tilde{H}$  such that  $\tilde{H}/(\widehat{F}_2 \cap \tilde{H}) \cong \mathcal{M}(H)$ , this means that  $\tilde{H}\widehat{F}_2 = N_G(H)\widehat{F}_2$ . Since  $\tilde{H} \subset N_G(H)$  for any model, this means that  $\tilde{H}N_{\widehat{F}_2}(H) = N_G(\tilde{H})$ . Also, since  $\tilde{H}$  is a model,

$$\tilde{H} \cap N_{\widehat{F}_2}(H) = \tilde{H} \cap \widehat{F}_2 = H$$

So a model defined over the field of moduli splits the exact sequence.  $\square$

As a corollary, we see that both regular dessins and dessins without automorphisms are defined over their fields of moduli.

**Corollary 2.3.10.** *Regular dessins and dessins without (nontrivial) automorphisms are defined over their fields of moduli.*

*Proof.* Take a dessin given by  $H < \widehat{F}_2$ . Recall, from the proof of proposition 1.5.2, that a dessin's automorphism group is  $N_{\widehat{F}_2}(H)$ . In the case where a dessin has no automorphisms, this group is 1, so the exact sequence in the last lemma becomes

$$1 \longrightarrow 1 \longrightarrow N_G(H)/H \longrightarrow \mathcal{M}(H) \longrightarrow 1$$

So it is automatically split.

On the other hand, if a dessin is regular,  $N_{\widehat{F}_2}(H) = H$ , so the sequence is

$$1 \longrightarrow \widehat{F}_2/H \longrightarrow N_G(H)/H \longrightarrow \mathcal{M}(H) \longrightarrow 1$$

In this case,  $N_G(H)$  contains  $\widehat{F}_2$ , so the sequence will be split because  $\text{Gal}(\mathcal{K}/\mathbb{Q}(t)) = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ltimes \widehat{F}_2$ . If we take  $\widetilde{H} = \mathcal{M}(H) \ltimes H$ , it will be the section we are looking for.  $\square$

These two results can be seen in Wolfart's survey [24], where he uses Theorem 1 in Weil's paper [23]. This Theorem, in our case, states the following.

**Proposition 2.3.11.** *A Belyi pair  $(C, f)$  is defined over its field of moduli  $\mathcal{M}(C, f)$  if and only if for every  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathcal{M}(C, f))$ , there is an isomorphism*

$$\varphi_\sigma : (C, f) \longrightarrow (C^\sigma, f^\sigma)$$

*Such that, for every  $\sigma, \tau \in \text{Gal}(\overline{\mathbb{Q}}/\mathcal{M}(C, f))$ , the following holds:*

$$\varphi_{\tau\sigma} = \varphi_\sigma^\tau \circ \varphi_\tau$$

If we look at this proposition closely, we can see that the condition is the same as the splitting of our exact sequence. Suppose we have a splitting for a subgroup  $H$ , with a model  $\widetilde{H}$ . Then, for every  $\sigma \in \mathcal{M}(H)$ , there is some  $g_\sigma \in \widehat{F}_2$  such that  $(\sigma, g_\sigma) \in \widetilde{H}$ . Recall that this  $g_\sigma$  had to verify that  $H^\sigma = g_\sigma H g_\sigma^{-1}$ . Therefore,

$$g_\sigma \left( \mathcal{K}^{H^\sigma} \right) = g_\sigma \left( \mathcal{K}^{g_\sigma H g_\sigma^{-1}} \right) = \mathcal{K}^H$$

So  $g_\sigma$  gives an isomorphism from  $\mathcal{K}^{H^\sigma}$  to  $\mathcal{K}^H$ . Also, the choice of  $g_\sigma$  doesn't change this isomorphism: take another  $g'_\sigma$ . Then,  $(g'_\sigma, \sigma)^{-1}(g_\sigma, \sigma) \in \widetilde{H} \cap \widehat{F}_2 = H$ , so, for some  $h \in \widehat{F}_2$ ,

$$(1, h) = \left( \sigma^{-1}, (g'_\sigma)^{-1} \sigma^{-1} \right) (\sigma, g_\sigma) = (1, g'^{-1}_\sigma g_\sigma)$$

So  $g_\sigma \in g'_\sigma H$ , or equivalently,  $g_\sigma \in g'_\sigma H g'^{-1}_\sigma g'_\sigma = H^\sigma g'_\sigma$ . Therefore,  $g_\sigma g'^{-1}_\sigma \in \text{Gal}(\mathcal{K}/\mathcal{K}^{H^\sigma})$ , so their actions on the field  $\mathcal{K}^{H^\sigma}$  are the same, i.e. for any  $f \in \mathcal{K}^{H^\sigma}$ ,  $f^{g_\sigma} = f^{g'_\sigma}$ .

If we define  $\varphi_\sigma$  to be the morphism from  $\overline{\mathbb{Q}}(C)$  to  $\overline{\mathbb{Q}}(C^\sigma)$  such that  $\varphi_\sigma^* = g_\sigma$ , then the condition is satisfied, as we can see.  $\widetilde{H}$  is a subgroup, so

$$(\tau\sigma, g_{\tau\sigma}) = (\tau, g_\tau)(\sigma, g_\sigma) = (\tau\sigma, g_\tau^\sigma g_\sigma)$$

So  $g_{\tau\sigma} = g_\tau^\sigma g_\sigma = g_\sigma \circ g_\tau^\sigma$ . If we make  $\varphi_\sigma = g_\sigma^*$ , and the same for  $\tau$ , we have that

$$\varphi_{\tau\sigma} = \varphi_\sigma^\tau \circ \varphi_\tau$$

Reciprocally, suppose such  $\varphi_\sigma$  exist. Then, we can follow this reasoning backwards to pick every  $g_\sigma$  for each  $\sigma \in \mathcal{M}(H)$ , such that  $\varphi_\sigma^* = g_\sigma|_{\overline{\mathbb{Q}}(C^\sigma)}$ . Then, the set

$$\{(\sigma, g_\sigma) : \sigma \in \mathcal{M}(H), \varphi_\sigma^* = g_\sigma|_{\overline{\mathbb{Q}}(C^\sigma)}\} \subset G$$

Will be a subgroup, because of the compatibility condition, and thus there will be a splitting of the sequence.



## 2.4 Dessins with one face

In this section we are going to prove the following.

**Theorem 2.4.1.** *Dessins d'enfants with one face are defined over their field of moduli.*

This is a slight generalization of the theorem that dessins that are trees embedded in  $\mathbb{P}^1$ , i.e. dessins with one face and genus 0, are defined over their field of moduli. This result can be found in [13], with a different proof than the one we are giving here. In the book, it says that the theorem was first published in [3], but it appeared earlier in some unpublished notes in Russian by Shabat for a seminar on dessins d'enfants. I have not read these notes, but apparently they used Galois cohomology, so his ideas are probably similar to the ones presented here.

Before we start with this, we are going to look at how the Galois group acts on ramified points.

Let us call  $\hat{P}$  the valuation of  $\mathcal{K}$  which restricts to  $P_H$  on every subfield  $\mathcal{K}^H$ . On each dessin,  $P_H$  lies on an edge (since we chose it to be a preimage of  $1/2$ , but it really doesn't matter). This edge lies in some white triangle, that is, we take the black and the white vertices that are its endpoints, and out of the two faces that contain the edge, we choose the one that has a star vertex that makes the vertices of the triangle be in counterclockwise order black-white-star, so that the triangle will be white. If, for each dessin, we choose these points as canonical preimages of 0, 1 and  $\infty$ , it is clear that, for example, for 0, we will obtain points  $\{Q_H\}_H$  compatible with the covers between dessins, so the family of points gives rise to a valuation in  $\mathcal{K}$ , which we can call  $\hat{P}_0$ . Similarly, we obtain  $\hat{P}_1$  and  $\hat{P}_\infty$ .

We are going to look at the stabilizer of  $\hat{P}_\infty$  in  $\hat{F}_2$ , by the action of  $\hat{F}_2$  on regular dessins. Note that, in every dessin, the monodromy action of  $z = (xy)^{-1}$  is a rotation around the face which contains  $P_\infty$ . Therefore, this stabilizer contains  $\langle z \rangle$ , the (closed) subgroup generated by  $z$ . Let us prove that this is the whole stabilizer.

Suppose that  $g \in \hat{F}_2$  fixes  $\hat{P}_\infty$ . Take a regular dessin given by  $H \triangleleft \hat{F}_2$ . The automorphism of  $D$  given by  $g$  maps  $P_H$  to some point  $g(P_H)$ , which must lie on one of the edges of the face that contains  $P_\infty$  for it to fix  $P_\infty$ . Thus,  $g(P_H) = z^m(P_H)$  for some  $m$ . Since the automorphism group of a dessin acts faithfully, it follows that  $g \equiv z^m \pmod{H}$ . Therefore,  $g$  is a power of  $z$  in every quotient  $\hat{F}_2/H$ , so it belongs to the closed group that  $z$  generates.

Note that this group is isomorphic to  $\hat{\mathbb{Z}}$ , so we can write things like  $z^n$ , where  $n \in \hat{\mathbb{Z}}$ . Also,  $\hat{\mathbb{Z}}$  has a natural ring structure.

**Proposition 2.4.2.** *Let  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , and let it act on  $\hat{F}_2$  on the way we have defined in theorem 2.3.2. Then, there exist  $g_x, g_y, g_z \in \hat{F}_2$  such that*

$$x^\sigma = g_x^{-1} x^\alpha g_x; y^\sigma = g_y^{-1} y^\alpha g_y; z^\sigma = g_z^{-1} z^\alpha g_z$$

Where  $\alpha \in \hat{\mathbb{Z}}$  is such that, for every root of unity  $\xi \in \overline{\mathbb{Q}}$ ,  $\xi^\sigma = \xi^\alpha$ .

*Proof.* Take some open  $H \triangleleft \hat{F}_2$ . We can assume, by passing to a smaller group that is contained in  $H$ , that it is invariant under the Galois action, by taking

$$\bigcap_{g \in G} H^g$$

This is clearly a normal subgroup and it is Galois invariant. There are also a finite number of different groups in the intersection, so it is of finite index. We are going to call this subgroup  $H$ , and note that its field of moduli is  $\mathbb{Q}$ , and, since it is regular, its field of definition is also  $\mathbb{Q}$ .

Call  $P_0$  the restriction of  $\hat{P}_0$  to the corresponding Galois extension, and  $P$  for the restriction of  $\hat{P}$ . We know that  $x(P_0) = P_0$ , where  $x$  is understood as an automorphism of the dessin. We have that

$$x^\sigma(P_0^\sigma) = (x(P_0))^\sigma = P_0^\sigma$$

So  $x^\sigma$  fixes  $P_0^\sigma$ . Let  $g$  be such that  $P_0^\sigma = g(P_0)$ , for some  $g \in \hat{F}_2/H$ . This  $g$  exists because the automorphism group acts transitively. Then,  $(x^\sigma)^g$  fixes  $P_0$ , so  $(x^\sigma)^g$  lies in the projection of the stabilizer of  $P_0$ , which is  $\langle x \rangle$ . Therefore, for some  $\alpha$ ,  $x^\sigma = (x^\alpha)^{g^{-1}}$ .

The same thing happens for  $y$  and  $z$ , taking the points corresponding to  $y$  and  $z$ . Now, let see what  $\alpha$  is, and that is indeed the same for  $x$ ,  $y$  and  $z$ .

Consider the point  $P_0$  and its valuation ring  $\mathcal{O}_{P_0}$ . Since the curve is smooth, it is a DVR, so the space  $\mathfrak{m}_{P_0}/\mathfrak{m}_{P_0}^2$  has dimension 1. Since the Belyi map on a neighborhood of  $P_0$  looks like  $z \mapsto z^m$ , where  $m$  is the order of  $x$  in  $\hat{F}_2/H$ , it follows that the map that  $x$  induces in the cotangent space  $\mathfrak{m}_{P_0}/\mathfrak{m}_{P_0}^2$  is given by  $f \mapsto \xi f$ , where  $\xi$  is a primitive  $m$ -th root of unity.

Take a function  $f$  that has valuation 1 in  $P_0$ , that is, if we call  $\mathfrak{m}_{P_0}$  the ideal of functions vanishing in  $P_0$ ,  $f$  belongs to  $\mathfrak{m}_{P_0}$  but not to  $\mathfrak{m}_{P_0}^2$ . If we apply  $x$ , we get another function  $f^x$ , that is also in  $\mathfrak{m}_{P_0}$ , because  $x$  fixes  $P_0$ , and  $f^x = \xi f \pmod{\mathfrak{m}_{P_0}^2}$ .

If we apply  $\sigma$  to everything, we have that  $f^{\tilde{\sigma}} \in \mathfrak{m}_{P_0^{\tilde{\sigma}}} \setminus \mathfrak{m}_{P_0^{\tilde{\sigma}}}^2$ , and, if  $\xi'$  is such that  $(f^{\tilde{\sigma}})^{x^\sigma} \equiv \xi' f^{\tilde{\sigma}} \pmod{\mathfrak{m}_{P_0^{\tilde{\sigma}}}^2}$ , then

$$(f^{\tilde{\sigma}})^{x^\sigma} + \mathfrak{m}_{P_0^{\tilde{\sigma}}}^2 = (f^x + \mathfrak{m}_{P_0}^2)^{\tilde{\sigma}} = (\xi f + \mathfrak{m}_{P_0}^2)^{\tilde{\sigma}} = \xi^\sigma f^{\tilde{\sigma}} + \mathfrak{m}_{P_0^{\tilde{\sigma}}}^2$$

So  $\xi' = \xi^\sigma$ . Therefore, the map that  $x^\sigma$  induces on the cotangent space at  $P_0^{\tilde{\sigma}}$  is  $f \mapsto \xi^\sigma f$ .

Now, we know that there is some  $g$  such that  $x^\sigma = (x^\alpha)^{g^{-1}}$ , and  $P_0^{\tilde{\sigma}} = g(P_0)$ . Then,

$$\begin{aligned} \xi^\sigma f^{\tilde{\sigma}} + \mathfrak{m}_{P_0^{\tilde{\sigma}}}^2 &= (f^{\tilde{\sigma}})^{x^\sigma} + \mathfrak{m}_{P_0^{\tilde{\sigma}}}^2 = (f^{\tilde{\sigma}})^{(x^\alpha)^{g^{-1}}} + \mathfrak{m}_{g(P_0)}^2 = (f^{\tilde{\sigma}})^{g(x^\alpha)^{g^{-1}}} + \mathfrak{m}_{g(P_0)}^2 = (f^{\tilde{\sigma}})^{g x^\alpha g^{-1}} + (\mathfrak{m}_{P_0}^2)^{g^{-1}} = \\ &= \left( ((f^{\tilde{\sigma}})^g)^{x^\alpha} + \mathfrak{m}_{P_0}^2 \right)^{g^{-1}} = \left( \xi^\alpha (f^{\tilde{\sigma}})^g + \mathfrak{m}_{P_0}^2 \right)^{g^{-1}} = \xi^\alpha f^{\tilde{\sigma}} + \mathfrak{m}_{g(P_0)}^2 \end{aligned}$$

Therefore,  $\xi^\sigma = \xi^\alpha$ , so  $\alpha$  has the value we claimed.

If we take every  $H$  that is normal in  $\hat{F}_2$  and is Galois invariant, we get two families  $\{g_H\}_H$  and  $\{\alpha_H\}$  such that  $x^\sigma \equiv (x^{\alpha_H})^{g_H} \pmod{H}$ . It is clear that these families will give rise to an element of  $\hat{F}_2$  and an element of  $\hat{\mathbb{Z}}$ , since it will follow from the fact that  $x^\sigma$  is an element of  $\hat{F}_2$ .  $\square$

In view of the previous proposition, let us define the (right)  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -module  $\hat{\mathbb{Z}}(1)$ . As a group, it is  $\hat{\mathbb{Z}}$ , and the action of some  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  is multiplication by  $\alpha_\sigma \in \hat{\mathbb{Z}}$ , where  $\alpha_\sigma$  is such that if we take a root of unity  $\xi \in \overline{\mathbb{Q}}$ ,  $\xi^\sigma = \xi^{\alpha_\sigma}$ .

Let us look at the group  $S_\infty = \{g \in G : g(\hat{P}_\infty) = \hat{P}_\infty\}$ . This is similar to what we did in theorem 2.3.2. There, we considered the subgroup that fixed one point, and it turned out to be a section of  $\text{Gal}(\mathcal{K}/\mathbb{Q}(t)) \rightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . Now, this group will turn out to be the semidirect product  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ltimes \hat{\mathbb{Z}}(1)$ , where  $\hat{\mathbb{Z}}(1)$  is the subgroup of  $\hat{F}_2$  generated by  $z$ . Since the stabilizer of  $P_\infty$  in  $\hat{F}_2$  is  $\langle z \rangle$ ,  $S_\infty \cap \hat{F}_2 = \langle z \rangle$ . Note that its image in  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  is the whole group: if  $g \in G$  maps  $z$  to  $(z^\alpha)^{g_z}$ , then  $gg_z^{-1}$  will belong to  $S_\infty$ .

Let us prove that this group is a semidirect product. Consider the group

$$A = \{g \in G : z^g \in \langle z \rangle, \exists u \in [\hat{F}_2, \hat{F}_2] \text{ such that } x^g \in \langle x \rangle^u\}$$

We are going to prove that  $A \cap \hat{F}_2 = 1$  and  $A\hat{F}_2 = G$ . In particular, it will follow that  $A \cap \langle z \rangle = 1$  and  $A\langle z \rangle = S_\infty$ .

$A$  is clearly a subgroup of  $G$ , so no comments there. Suppose  $g \in A \cap \hat{F}_2$ . Then,  $z^g$  must equal  $z$ , since  $z$  is not conjugate to any of its powers: it is not conjugate in the quotient  $\hat{F}_2/\langle\langle x \rangle\rangle \cong \hat{\mathbb{Z}}$ , so it can't be conjugate in  $\hat{F}_2$ . Therefore,  $g$  commutes with  $z$ . Since the centralizer of  $z$  in  $\hat{F}_2$  is  $\langle z \rangle$  (see [12]), it follows that  $g \in \langle z \rangle$ . But then, we must have, for some  $\alpha, \beta \in \hat{\mathbb{Z}}$  and  $u \in [\hat{F}_2, \hat{F}_2]$ ,  $x^g = x^{z^\beta} = (x^\alpha)^u$ . This, as before, implies that  $uz^{-\beta} \in \langle x \rangle$ , so  $u$  must equal  $x^\gamma z^\beta$ . For  $u$  to be in  $[\hat{F}_2, \hat{F}_2]$ ,  $\beta$  and  $\gamma$  must equal 0, and  $\alpha$  must equal 1, so  $g = 1$ .

Let us see that  $A\hat{F}_2 = G$ . Take some  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . We know that there is some  $\alpha \in \hat{\mathbb{Z}}$  and some  $g_z, g_x \in \hat{F}_2$  such that

$$z^\sigma = (z^\alpha)^{g_z}; x^\sigma = (x^\alpha)^{g_x}$$

Take  $\sigma' = \sigma g_z^{-1} z^\beta$ . Then,

$$z^{\sigma'} = z^\alpha; x^{\sigma'} = (x^\alpha)^{g_x g_z^{-1} z^\beta} = (x^\alpha)^{x^\gamma g_x g_z^{-1} z^\beta}$$

It is clear that we can pick some  $\gamma, \beta \in \hat{\mathbb{Z}}$  so that

$$x^\gamma g_x g_z^{-1} z^\beta \in [\hat{F}_2, \hat{F}_2]$$

So, for this  $\beta$ ,  $\sigma' g_z^{-1} z^\beta$  belongs to  $A$ . It follows that  $A$  intersects every class in  $G/\hat{F}_2 = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , so  $A\hat{F}_2 = G$ , as we wanted. It follows that  $A$  gives a section of

$$1 \longrightarrow \hat{F}_2 \longrightarrow G \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow 1$$

In particular,  $A \cong \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . If we look at the group  $S_\infty = A\langle z \rangle$ , we see that it is a semidirect product and, by proposition 2.4.2, it is isomorphic to the semidirect product  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ltimes \hat{\mathbb{Z}}(1)$ .

We are going to use a lemma to prove that every dessin with one face is defined over its field of moduli. We will prove it at the end of the section.

**Lemma 2.4.3.** *Let  $U$  be an open subgroup of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ltimes \widehat{\mathbb{Z}}(1)$ . Then, there exist a subgroup  $T < U$ , a number field  $K$  and an integer  $m$  such that*

- $T \cap m\widehat{\mathbb{Z}}(1) = 1$
- $T(m\widehat{\mathbb{Z}}(1)) = U$
- $T \cong \text{Gal}(\overline{\mathbb{Q}}/K)$

Let us prove the main theorem, and leave this lemma for later.

**Theorem 2.4.4.** *Every dessin with one face is defined over its field of moduli.*

*Proof.* Let the dessin be given by an open subgroup  $H < \widehat{F}_2$ . The fact that it has one face means that  $z$  acts transitively on the edges, i.e. it acts transitively on the cosets of  $H$ , so  $\langle z \rangle H = \widehat{F}_2$ .

Now, as we know, the field of moduli of the dessin is the fixed field of  $\mathcal{M}(H)$ , the image in  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  of  $N_G(\widehat{F}_2)$ . Consider now the group  $A$  as previously defined. Take  $U = N_G(H) \cap S_\infty = N_G(H) \cap A\langle z \rangle$ .

Since  $U$  is open, applying lemma 2.4.3, we see that  $U = T\langle z^m \rangle$  for some  $m$ , where  $T \cap \langle z \rangle = 1$  and  $T\langle z \rangle = U$ . Since  $T \cap \langle z \rangle = 1$  and  $T \cap \widehat{F}_2 \subset A\langle z \rangle \cap \widehat{F}_2 = \langle z \rangle$ , it follows that  $T \cap \widehat{F}_2 = 1$ .

Also, let us prove that the image of  $T$  in  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  is  $\mathcal{M}(H)$ . Suppose  $\sigma \in \mathcal{M}(H)$ . Then, we can take its unique representative  $\sigma' \in A$ , and for some  $g \in \widehat{F}_2$ ,  $\sigma'g$  will be in  $N_G(H)$ . Now, every coset of  $N_{\widehat{F}_2}(H)$  is  $z^l N_{\widehat{F}_2}(H)$  for some  $l$ ; so  $\sigma'z^l$  will also be in  $N_G(H)$ . Since  $\sigma'z^l \in A\langle z \rangle$ , it is in  $N_G(H) \cap A\langle z \rangle = U$ . Therefore, the image of  $U$  in  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  is  $\mathcal{M}(H)$ . Since the images of  $U$  and  $T$  in  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  are the same (because  $U = T\langle z \rangle$ ), the image of  $T$  is also  $\mathcal{M}(H)$ . So  $T\widehat{F}_2 = N_G(H)\widehat{F}_2$ , and  $TN_{\widehat{F}_2}(H) = N_G(H)$ .

So  $T$  satisfies the following:

$$T \cap \widehat{F}_2 = 1; T\widehat{F}_2 = N_G(H)\widehat{F}_2$$

Therefore, if we take  $\widehat{H} = TH$ , we will have that

$$\widehat{H} \cap \widehat{F}_2 = H; \widehat{H}N_{\widehat{F}_2}(H) = N_G(H)$$

And this is precisely the characterization of  $H$  being definable over its field of moduli, by proposition 2.3.9.  $\square$

Let us prove lemma 2.4.3. To do it, we are going to use some cohomology of groups, such as the relationship between  $H^2$  and extensions, Hilbert's Theorem 90 and the long exact sequence in cohomology. For a reference about these facts, see [19]. Suppose we have some open subgroup  $U$  in  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ltimes \widehat{\mathbb{Z}}(1)$ . Its intersection with  $\widehat{\mathbb{Z}}(1)$  is an open subgroup, so it equals  $m\widehat{\mathbb{Z}}(1)$  for some  $m$ . Let  $K$  be such that the image of  $U$  in  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  equals  $\text{Gal}(\overline{\mathbb{Q}}/K)$ . Then, we have an exact sequence

$$1 \longrightarrow m\widehat{\mathbb{Z}}(1) \longrightarrow U \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow 1$$

We want to prove that it is split. If it is split, then the section  $T$  of  $\text{Gal}(\overline{\mathbb{Q}}/K)$  will be the group we are looking for and the result will be proven.

**Lemma 2.4.5.** *For every  $l \in \mathbb{N}$ , the following sequence splits:*

$$1 \longrightarrow \frac{m\widehat{\mathbb{Z}}(1)}{ml\widehat{\mathbb{Z}}(1)} \longrightarrow \frac{U}{ml\widehat{\mathbb{Z}}(1)} \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow 1$$

*Proof.* The first group in the sequence is the cyclic group  $C_l$ , with the same module structure as the group  $\mu_l$  of  $l$ -th roots of unity. Let  $\varphi \in H^2(\text{Gal}(\overline{\mathbb{Q}}/K), \mu_l)$  be the cocycle associated to this extension. Consider the sequence

$$1 \longrightarrow \frac{\widehat{\mathbb{Z}}(1)}{ml\widehat{\mathbb{Z}}(1)} \longrightarrow \frac{\text{Gal}(\overline{\mathbb{Q}}/K) \ltimes \widehat{\mathbb{Z}}(1)}{ml\widehat{\mathbb{Z}}(1)} \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow 1$$

It is clearly split because a section is just restricting the section of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ltimes \widehat{\mathbb{Z}}(1)$  to  $\text{Gal}(\overline{\mathbb{Q}}/K)$ . Also, the inclusion  $i : \frac{m\widehat{\mathbb{Z}}(1)}{ml\widehat{\mathbb{Z}}(1)} \longrightarrow \frac{\widehat{\mathbb{Z}}(1)}{ml\widehat{\mathbb{Z}}(1)} \cong \mu_{ml}$  induces a map  $i_* : H^2(\text{Gal}(\overline{\mathbb{Q}}/K), \mu_l) \longrightarrow H^2(\text{Gal}(\overline{\mathbb{Q}}/K), \mu_{ml})$ , and  $i_*(\varphi)$  is the cocycle corresponding to this second extension. Since the extension is split,  $i_*(\varphi) = 1$  in the cohomology group.

Now, we claim that  $i_*$  is injective. From this, it will follow that the cocycle for the first extension was 1, and therefore the extension also splits. Take the exact sequence

$$1 \longrightarrow \mu_l \longrightarrow \overline{\mathbb{Q}}^\times \xrightarrow{\cdot l} \overline{\mathbb{Q}}^\times \longrightarrow 1$$

For this exact sequence, take the long exact sequence in cohomology, which goes

$$\cdots \longrightarrow H^1(\text{Gal}(\overline{\mathbb{Q}}/K), \overline{\mathbb{Q}}^\times) \longrightarrow H^2(\text{Gal}(\overline{\mathbb{Q}}/K), \mu_l) \longrightarrow H^2(\text{Gal}(\overline{\mathbb{Q}}/K), \overline{\mathbb{Q}}^\times) \longrightarrow \cdots$$

Hilbert's Theorem 90 states that for any field  $K$ ,  $H^1(\text{Gal}(\overline{K}/K), \overline{K}^\times) = 0$ . Therefore, the map that goes from  $H^2(\text{Gal}(\overline{\mathbb{Q}}/K), \mu_{ml})$  to  $H^2(\text{Gal}(\overline{\mathbb{Q}}/K), \overline{\mathbb{Q}}^\times)$  is injective. In particular, since it is the composition of the following two maps:

$$H^2(\text{Gal}(\overline{\mathbb{Q}}/K), \mu_l) \longrightarrow H^2(\text{Gal}(\overline{\mathbb{Q}}/K), \mu_{ml}) \longrightarrow H^2(\text{Gal}(\overline{\mathbb{Q}}/K), \overline{\mathbb{Q}}^\times)$$

The first map is also injective. This is what we wanted to prove, since this map is  $i_*$ . Therefore the cocycle  $\varphi$  is 0 in  $H^2(\text{Gal}(\overline{\mathbb{Q}}/K), \mu_l)$ .  $\square$

We have proven that for every  $l$ , the following sequence splits:

$$1 \longrightarrow \frac{m\widehat{\mathbb{Z}}(1)}{ml\widehat{\mathbb{Z}}(1)} \longrightarrow \frac{U}{ml\widehat{\mathbb{Z}}(1)} \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow 1$$

Let  $s_l : \text{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow \frac{U}{ml\widehat{\mathbb{Z}}(1)}$  be a section. We need to prove that there is a section  $s : \text{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow U$ . Of course, if the image of every other section of the form  $s_{lk}$  in the quotient  $\frac{U}{ml\widehat{\mathbb{Z}}(1)}$  was  $s_l$ , our job would be done. So what we need to do is construct such compatible sections.

Take a section  $s_{lk} : \text{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow \frac{U}{mlk\widehat{\mathbb{Z}}(1)}$ , and let  $\overline{s_{lk}}$  be its image in the quotient  $\frac{U}{ml\widehat{\mathbb{Z}}(1)}$ , i.e. if  $\pi$  is the projection,  $\overline{s_{lk}} = \pi \circ s_{lk}$ .  $\overline{s_{lk}}$  is also a section of the sequence for  $l$ , so let us see the relation between  $s_l$  and  $\overline{s_{lk}}$ . For every  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/K)$ ,  $s_l(\sigma)$  and  $\overline{s_{lk}}(\sigma)$  are in the same coset of  $\mu_l$ , so there is some  $\alpha(\sigma) \in \mu_l$  such that

$$\overline{s_{lk}}(\sigma) = s_l(\sigma)\alpha(\sigma)$$

Now, both  $s_l$  and  $\overline{s_{lk}}$  are group homomorphisms, so, for  $\sigma, \tau \in \text{Gal}(\overline{\mathbb{Q}}/K)$ ,

$$s_l(\sigma\tau)\alpha(\sigma\tau) = \overline{s_{lk}}(\sigma\tau) = \overline{s_{lk}}(\sigma)\overline{s_{lk}}(\tau) = s_l(\sigma)\alpha(\sigma)s_l(\tau)\alpha(\tau) = s_l(\sigma)s_l(\tau)\alpha(\sigma)^{s_l(\tau)}\alpha(\tau) = s_l(\sigma\tau)\alpha(\sigma)^{s_l(\tau)}\alpha(\tau)$$

Since  $\text{Gal}(\overline{\mathbb{Q}}/K)$  acts as automorphisms of  $\mu_l$ ,  $\alpha(\sigma)^{s_l(\tau)} = \alpha(\sigma)^\tau$ , and what we have is

$$\alpha(\sigma\tau) = \alpha(\sigma)^\tau \alpha(\tau)$$

This means that  $\alpha$  is a cocycle in  $H^1(\text{Gal}(\overline{\mathbb{Q}}/K), \mu_l)$ . This cohomology group is not 0, but  $H^1(\text{Gal}(\overline{\mathbb{Q}}/K), \overline{\mathbb{Q}}^\times)$  is, by Theorem 90. Therefore, in  $H^1(\text{Gal}(\overline{\mathbb{Q}}/K), \overline{\mathbb{Q}}^\times)$ , the cocycle  $\alpha$  is indeed 0; so there exists some  $\beta' \in \overline{\mathbb{Q}}$  such that  $\alpha(\sigma) = \beta'^\sigma / \beta'$ . Now, take some  $\beta \in \overline{\mathbb{Q}}$  such that  $\beta^{-k} = \beta'$ , and define

$$s'_{lk}(\sigma) = s_{lk}(\sigma)\beta^\sigma / \beta$$

Note that  $\beta^\sigma / \beta$  lies in  $\mu_{lk}$ . Let us check two things: that  $s'_{lk}$  is another section, and that its projection  $\overline{s'_{lk}}$  equals  $s_l$ .

Since  $\beta^\sigma / \beta \in \mu_{lk}$ , it is clear that  $s'_{lk} = s_{lk}$  modulo  $m\widehat{\mathbb{Z}}(1)$ , so there is no problem there. We only need to check that it is a homomorphism. Let  $\sigma, \tau \in \text{Gal}(\overline{\mathbb{Q}}/K)$ . Then

$$s'_{lk}(\sigma)s'_{lk}(\tau) = s_{lk}(\sigma)\frac{\beta^\sigma}{\beta}s_{lk}(\tau)\frac{\beta^\tau}{\beta} = s_{lk}(\sigma)s_{lk}(\tau)\left(\frac{\beta^\sigma}{\beta}\right)^\tau \frac{\beta^\tau}{\beta} = s_{lk}(\sigma)s_{lk}(\tau)\frac{\beta^{\sigma\tau}}{\beta^\tau}\frac{\beta^\tau}{\beta} = s_{lk}(\sigma\tau)\frac{\beta^{\sigma\tau}}{\beta} = s'_{lk}(\sigma\tau)$$

For the second part, let us check that  $\overline{s'_{lk}} = s_l$ . Note that the projection  $\frac{m\widehat{\mathbb{Z}}(1)}{mlk\widehat{\mathbb{Z}}(1)} \longrightarrow \frac{m\widehat{\mathbb{Z}}(1)}{ml\widehat{\mathbb{Z}}(1)}$  can be given by  $\xi \mapsto \xi^k$ .

$$\overline{s'_{lk}}(\sigma) = \overline{s_{lk}}(\sigma)\left(\frac{\beta^\sigma}{\beta}\right)^k = \overline{s_{lk}}(\sigma)\alpha(\sigma)^{-1} = s_l(\sigma)$$

So  $s'_{lk}$  is a section that projects to  $s_l$ . We can continue doing this for bigger  $k$ 's, and we will obtain a compatible sequence of sections, which will yield a section of

$$1 \longrightarrow m\widehat{\mathbb{Z}}(1) \longrightarrow U \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow 1$$

As we wanted in the first place. This concludes the proof of lemma 2.4.3.

## 2.5 A dessin that is not defined over its field of moduli

We are going to give an example of a dessin that isn't defined over its field of moduli, following [4].

The easiest field where we can prove that a dessin isn't defined is  $\mathbb{R}$ . Let us see how complex conjugation acts on  $\widehat{F}_2$  when we embed  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  in  $\text{Aut}(\widehat{F}_2)$ . Conjugation is a continuous map: therefore, it maps the fundamental group of  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$  to itself. By this homomorphism,  $x$ , the path that goes around 0 is mapped to  $x^{-1}$  and  $y$  is mapped to  $y^{-1}$ .

Take a Belyi pair  $(C, f)$ , with a base point  $P$ . Let  $P^x$  be the monodromy action of  $x \in F_2 = \pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\})$  on  $P$ . Then, if we look at the conjugate Belyi pair  $(\overline{C}, \overline{f})$  (conjugate in the sense of complex conjugation), the point  $\overline{P}^x$  will be determined, as usual, by the lifting of  $x$  to  $\overline{C}$ . Now, we just need to note that  $\overline{C}$  is homeomorphic to  $C$ , that  $\overline{f}$  equals  $f$  composed with conjugation in  $\mathbb{P}^1$ . Thus, we have the following commutative diagram, if we call conjugation  $c$ , and we use  $\widetilde{x^{-1}}$  for the lifting of  $x^{-1}$  to  $C$ .

$$\begin{array}{ccc}
 & C & \\
 \widetilde{x^{-1}} \nearrow & \downarrow f & \\
 [0, 1] & \xrightarrow{x^{-1}} & \mathbb{P}^1 \\
 x \searrow & \downarrow c & \\
 & \mathbb{P}^1 & \\
 & \nwarrow \overline{f} & 
 \end{array}$$

Therefore, the path  $x$  will lift to the same path in  $\overline{C}$  that  $x^{-1}$  lifts to in  $C$ . Since, if we identify  $C$  with  $\overline{C}$ , we have that  $\overline{f} = c \circ f$ , then  $x = c \circ f \circ \widetilde{x^{-1}} = \overline{f} \circ \widetilde{x^{-1}}$ . Therefore,  $\overline{P}^x = P^{x^{-1}}$ , if we identify  $C$  with  $\overline{C}$ .

In conclusion, the automorphism induced by  $c$ , the conjugation, in  $\widehat{F}_2$  is given by

$$x \mapsto x^{-1}$$

$$y \mapsto y^{-1}$$

Take a dessin given by an open subgroup  $H < \widehat{F}_2$ . Its moduli field is real if it is fixed by the conjugation  $c$ . Suppose we number the points on the dessin  $P_1, \dots, P_n$ . Let  $s_x$  and  $s_y$  be the permutations such that  $P_i^x = P_{s_x(i)}$ . Then, we have that

$$(P_i^c)^x = (P_i^{x^{-1}})^c = (P_i^x)^c = P_{i^{s_x}^{-1}}^c$$

So the permutation  $x$  induces on the conjugate dessin is  $s_x^{-1}$ , and similarly for  $y$ .

Suppose there is an isomorphism  $\varphi : (C, f) \rightarrow (\overline{C}, \overline{f})$ . This isomorphism is determined by the image of a point, so it is equivalent to a permutation  $\omega \in S_n$  defined in the following way:

$$\varphi(P_i) = P_{i^\omega}^c$$

For  $\varphi$  to be an isomorphism, it is required that it commute with the action of  $x$ , that is,  $\varphi(P_i^x) = \varphi(P_i)^x$ . This, in terms of  $\omega$ , is  $x\omega = \omega x^{-1}$ . Therefore,  $x^{-1} = x^\omega$ .

Now, suppose a dessin has a real model  $\widehat{H}$ . Then the image of  $\widehat{H}$  in  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  is the Galois group of a real field, so it contains  $c$ . Therefore, there will be some  $c' \in \widehat{H}$  such that its image in  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  is  $c$ . Since  $c$  has order 2,  $c'^2$  will lie in  $\widehat{F}_2$ . Also,  $c'^2 \in \widehat{H}$ , and since  $\widehat{H} \cap \widehat{F}_2 = H$ ,  $c'^2$  must lie in  $H$ .

Suppose  $c' = (c, g)$ . Then,  $c'^2 \in H$  means that

$$c'^2 = (c, g)(c, g) = (c^2, g^c g) = (1, g^c g) \in H$$

So we must have that  $g^c g \in H$ . In terms of permutations, it means that  $g^c g$  acts on the edges of  $H$  as the identity. Let us see what this means:  $g$  maps  $H^c$  to  $H$ , so it maps  $\mathcal{K}^{H^c}$  to  $\mathcal{K}^H$ . Therefore, the corresponding morphism of dessins maps  $(C, f)$  to  $(\overline{C}, \overline{f})$ , so we get a permutation  $\omega \in S_n$  as before, given by

$$\varphi(P_i) = P_{i^\omega}^c$$

Now,  $g^c$  maps  $(\overline{C}, \overline{f})$  to  $(C, f)$ , and it is given by

$$\varphi^c(P_i^c) = (\varphi(P_i))^c = P_{i^\omega}^{c^2} = P_{i^\omega}$$

So, for us to have that  $g^c g \in H$ , we must have that  $\varphi^c \circ \varphi = 1$ , so, for every point,

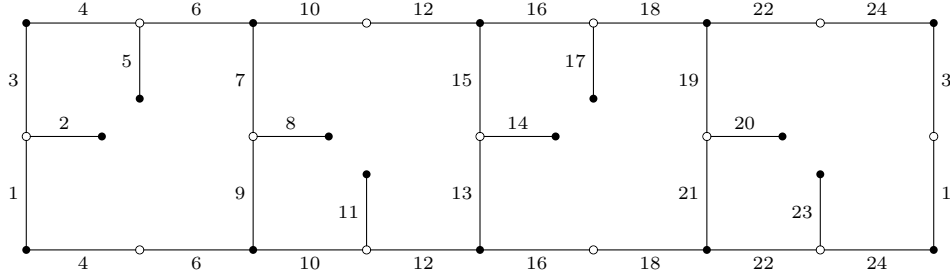
$$P_i = \varphi^c(\varphi(P_i)) = \varphi^c(P_{i\omega}) = P_{i\omega^2}$$

In other words,  $\omega$  must have order 2.

Therefore, we have the following, which is theorem 2 in [4].

**Proposition 2.5.1.** *Let a dessin d'enfant be given by its cartographic group  $\langle x, y \rangle < S_n$ . Then, the dessin's field of moduli is real if and only if there exists some  $\omega \in S_n$  such that  $x^\omega = x^{-1}$  and  $y^\omega = y^{-1}$ . The dessin can be defined over a real field if and only if this  $\omega$  can be chosen of order 2.*

It is relatively easy then to give dessins that are invariant under conjugation but are not defined over the reals. For example, take the following dessin on a curve of genus 1. The opposing sides of the rectangle are identified.



This dessin has the following monodromy action, as it is seen from the picture:

$$x \mapsto (4, 1, 24, 3)(9, 6, 7, 10)(16, 13, 12, 15)(21, 18, 19, 22)$$

$$y \mapsto (1, 2, 3)(4, 5, 6)(9, 8, 7)(12, 11, 10)(13, 14, 15)(16, 17, 18)(21, 20, 19)(24, 23, 22)$$

It clearly has an automorphism of order 2, given by sending the edges numbered  $i$  to  $i + 12$ . Also, we have that, if we take

$$\omega = (1, 7, 13, 19)(2, 8, 14, 20)(3, 9, 15, 21)(4, 10, 16, 22)(5, 11, 17, 23)(6, 12, 18, 24)$$

Conjugation by  $\omega$  sends  $x$  to  $x^{-1}$  and  $y$  to  $y^{-1}$ . In particular,  $c$  leaves the dessin invariant, so its field of moduli is real. However,  $\omega$  has order 4, and if there is another  $\omega'$  such that  $x^\omega = x^{-1}$  and  $y^\omega = y^{-1}$ , then

$$x^\omega = x^{-1} = x^{\omega'}$$

And the same for  $y$ . Therefore,  $\omega\omega'^{-1}$  is an automorphism of the dessin. So any other  $\omega'$  is of the form  $g\varphi$ , where  $g$  is an automorphism. The only nontrivial automorphism is the one sending  $i$  to  $i + 12$ , and we can check that this composed with  $\omega$  equals  $\omega^{-1}$ .

Therefore, we have an example of a dessin that is not defined over its field of moduli.

## Part 3

# A regular dessin whose field of moduli is $\mathbb{Q}(\sqrt[3]{2})$

In this part we are going to give an example of a regular dessin d'enfant whose field of moduli is  $\mathbb{Q}(\sqrt[3]{2})$ . This is an example of a regular dessin whose field of moduli is not an abelian extension of  $\mathbb{Q}$ , thus answering a question in [2].

The way we are going to do this is as follows: we are going to explicitly construct a dessin on the elliptic curve  $C = V(Y^2 - X(X-1)(X - \sqrt[3]{2}))$ . Then, we are going to consider its regular cover and we are going to prove that when a Galois automorphism  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  doesn't fix  $\sqrt[3]{2}$ , it doesn't fix this regular cover either. This cover has genus 145. Then, we are going to consider a dessin which is covered by this one, so it is somewhat simpler (it has genus 61), and it also has the same field of moduli. We are also going to give an explicit description for the field of functions of this last dessin. Finally, we are going to prove that the underlying curve for this dessin also has the same field of moduli.

There is another example of a regular dessin with non-abelian cubic field of moduli. It is the regular cover of a dessin described by Shabat and Voevodsky in [21] and by Malle in [14]. In the last section, we will expand on this example.

### 3.1 A dessin $D_0$ over an elliptic curve

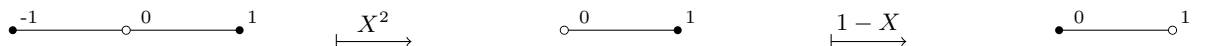
Let us define a dessin on the elliptic curve given by the equation  $Y^2 = X(X-1)(X - \sqrt[3]{2})$ . The dessin we are going to give is also described in [24].

Consider the map on  $C$  given by  $(X, Y) \mapsto X$ , or, in homogeneous coordinates,  $(X : Y : Z) \mapsto (X : Z)$ . This map is ramified at four points:  $(0 : 0 : 1)$ ,  $(1 : 0 : 1)$ ,  $(\sqrt[3]{2} : 0 : 1)$  and the point at infinity,  $(0 : 1 : 0)$ . Their images are  $\{0, 1, \sqrt[3]{2}, \infty\} \subset \mathbb{P}^1$ . In order to have a Belyi map for  $C$ , we need a map which is only ramified over 3 points. To do this, we are going to mirror the proof we gave for Belyi's theorem, in section 2.2.1: we compose with the map  $X \mapsto X^3$ , which ramifies only over 0 and  $\infty$ , and maps the points  $\{0, 1, \sqrt[3]{2}, \infty\}$  to  $\{0, 1, 2, \infty\}$ . Then, we compose with the map  $X \mapsto (X-1)^2$ , which ramifies over 0 and  $\infty$  and maps  $\{0, 1, 2, \infty\}$  to  $\{0, 1, \infty\}$ . Finally we will compose with  $X \mapsto 1 - X$  because it is more pleasant to have 0 mapped to 0 and 1 mapped to 1.

We now have a Belyi map  $f : C \mapsto \mathbb{P}^1$ , which is given by the composition of all the maps we have mentioned above: it is given by  $f(X, Y) = 1 - (X^3 - 1)^2$ , or equivalently, by  $f(X : Y : Z) = (Z^6 - (X^3 - Z^3)^2 : Z^6)$ . In order to be able to draw the dessin d'enfant corresponding to  $f$ , we need to know  $f^{-1}([0, 1])$ . Let us do this step by step. We will use the usual notation for dessins d'enfants: a black dot will represent a point in the preimage of 0 and a white point will represent one in the preimage of 1. The starting picture, just the segment  $[0, 1]$ , would look something like this:



Now, the map  $X \mapsto 1 - X$  just flips the segment, so its preimage is the same picture with the black and white dots interchanged. The map  $X \mapsto X^2$  looks like this:



Now, we have to compose with the map  $X^3$ . This map is ramified three times at 0. Here,  $\xi$  is the cubic root of unity  $\frac{-1+i\sqrt{3}}{2}$ :

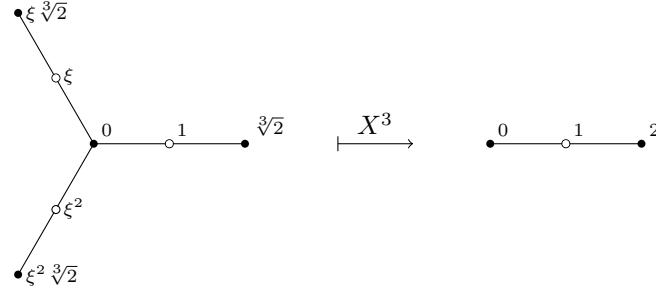


Figure 3.1: The dessin corresponding to  $X \mapsto 1 - (X^3 - 1)^2$ .

Finally, we need the preimage of this graph on the curve  $C$  by the projection on the first coordinate to know what the dessin looks like. The projection has degree 2 and it is ramified over 0, 1,  $\sqrt[3]{2}$  and  $\infty$ . Since it is ramified at  $\infty$ , it has only one face. We would like to know the ordering of the edges around that face. To do this, call the canonical generators of the fundamental group of  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$   $x$  and  $y$ . Recall that the monodromy action on the edges of  $x$  consists on rotating counterclockwise around black vertices, and the action of  $y$  consists on rotating counterclockwise around white vertices. Therefore,  $xy$  will consist on rotating clockwise around a face (we adopt the convention that the monodromy group acts on the right, so  $xy$  means  $x$  then  $y$ ). Therefore, if we number the edges in figure 3.1 like so:

Endpoints	Label	Endpoints	Label
0 – 1	1	1 – $\sqrt[3]{2}$	2
0 – $\xi$	3	1 – $\xi\sqrt[3]{2}$	4
0 – $\xi^2$	5	1 – $\xi^2\sqrt[3]{2}$	6

The action of  $x$  corresponds to the permutation (135), that of  $y$  corresponds to (12)(34)(56), and  $xy$  corresponds to (143652). Now, the dessin we are looking at has a monodromy action that factors through this one. We can number its edges  $1, \dots, 6, 1', \dots, 6'$ . Then, since  $xy$  has order 12 because the action is ramified at  $\infty$ , it must correspond, with appropriate labeling, to

$$z \mapsto (1436521'4'3'6'5'2')$$

So, the face of the dessin will look like figure 3.2. The labels for the vertices mark their image by the map  $(X, Y) \mapsto X$ .

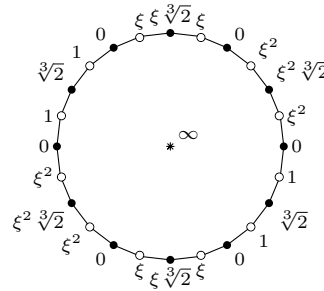


Figure 3.2: The labels mark the  $x$  coordinate of the points

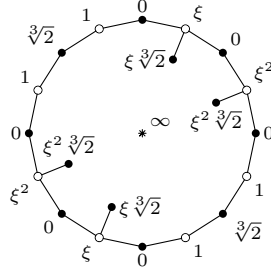
The vertices of the face are the preimages of  $\{0, 1, \xi, \xi^2, \sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2}\}$ . Some of the points, namely  $\xi, \xi^2, \xi\sqrt[3]{2}$  and  $\xi^2\sqrt[3]{2}$  have two different preimages and nonetheless these have the same label in the figure, because we are only labeling the  $X$  coordinates, for simplicity. Note that the points are in the same order as in the dessin in figure 3.1.

The dessin corresponding to  $(C, f)$  is figure 3.2 with some of its edges identified. What we are going to do now is figure out how the edges are identified. Since the curve is an orientable surface, the edges in the figure

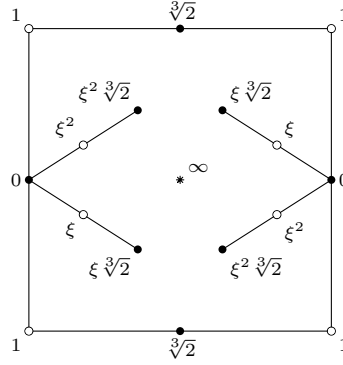


are identified in pairs, and the first coordinates of two identified edges must coincide. This leaves for each edge only two possibilities as to which edge it is identified with: take, for instance, the edges with endpoints marked 0 and 1, of which there are four. They are oriented in two different ways: two of them have endpoints  $0 \rightarrow 1$  in clockwise order, and the other two have endpoints  $1 \rightarrow 0$ . Two edges with the same orientation cannot be identified, for the resulting surface must be orientable: therefore, each of the edges is identified with one of the other two which have the opposite orientation, which gives two possibilities for the way they are identified.

Now, if we look at the points over  $\xi \sqrt[3]{2}$ , we know that these are not ramified, so there must be two of them. There are two ways of identifying the edges marked  $\xi - \xi \sqrt[3]{2}$ , but the one identifying the non-adjacent ones gives only one preimage of  $\xi \sqrt[3]{2}$ , which is not the case. Therefore, the adjacent edges must be identified, and the same thing happens for  $\xi^2 \sqrt[3]{2}$ . With the corresponding edges identified, the dessin must look like the following:



The same kind of reasoning applies to the points over  $\xi$  and  $\xi^2$ , so the resulting figure is



If we look at the remaining edges, we can see that for 0, 1 and  $\sqrt[3]{2}$  to have one preimage each, there is just one way in which they can be identified, which is by identifying opposite sides of the square (note that this agrees with the fact that the curve has genus 1).

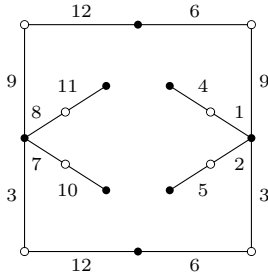


Figure 3.3: The dessin  $D_0$  with a numbering on its edges

We want to look at this dessin's regular cover. In order to do that, we will look at its cartographic group (recall that the cartographic group of a dessin is the automorphism group of its regular cover, proposition 1.5.4). To be able to present it as a permutation group by its action on the edges of the dessin, we will number them as in figure 3.3.

With this numbering, the cartographic group is generated by  $x = (1, 2, 3, 7, 8, 9)(6, 12)$ ,  $y = (1, 4)(2, 5)(7, 10)(8, 11)(3, 6, 9, 12)$  and  $z = (xy)^{-1} = (2, 5, 1, 4, 9, 12, 8, 11, 7, 10, 3, 6)$  (we adopt the convention that the cartographic group acts on the right).

If we see the dessin as a subgroup  $D_0$  of  $\widehat{F}_2$ , it is the stabilizer of an edge in the dessin (any edge, since the action is transitive, and thus any two stabilizers are conjugate).

If we take the edge marked 1, the stabilizer is the closure of the free group freely generated by

$$\langle x^6, y^2, (y^x)^4, (y^{x^2})^2, (y^{x^3})^2, (y^{x^5})^2, x^y, (x^{yx})^2, x^{yx^2}, x^{yx^3}, x^{yx^5}, x^2 y^2 x, x^{-1} y^{-1} x^{-1} y^{-1} x \rangle$$

(Note the convention that the cartographic group acts on the right, and that  $a^b$  means  $b^{-1}ab$ ). These generators are obtained as the generators for the fundamental group of the elliptic curve without the ramified points (recall that the subgroup associated to a cover is the pushforward of the fundamental group of the covering space, see section 1.3). The elliptic curve without the ramification points is a torus with 12 points removed, which has fundamental group  $F_{13}$ . Each of the generators corresponds to a loop going around one of the points, except for the last two, which are the loops that generate the fundamental group of the torus. Then, its preimage in  $\widehat{F}_2$  is the same as its closure. Nonetheless, we won't need this presentation, and we will be able to obtain a nicer one.

We are interested in the regular cover  $\widetilde{D}_0$  of the dessin. Recall that the regular cover is given by  $\widetilde{D}_0 = \text{Core}_{\widehat{F}_2} D_0$ . The quotient  $\widehat{F}_2 / \widetilde{D}_0$  is then the cartographic group of the dessin, so  $\widetilde{D}_0$  is the set of relations defining this group. We will call this group  $\mathcal{C} \cong \widehat{F}_2 / \widetilde{D}_0$ .

We will see that this dessin  $\widetilde{D}_0$  has  $\mathbb{Q}(\sqrt[3]{2})$  as field of moduli, by finding out also about the cartographic groups of its Galois conjugates, and seeing that they have different sets of relations.

### 3.2 The cartographic group of $D_0$

The cartographic group of  $D_0$  is the group  $\widehat{F}_2 / \widetilde{D}_0$ , and, since it acts faithfully on the edges of  $D_0$ , we can see it as the permutation group

$$\mathcal{C} = \langle x = (1, 2, 3, 7, 8, 9)(6, 12), y = (1, 4)(2, 5)(7, 10)(8, 11)(3, 6, 9, 12) \rangle < S_{12}$$

The first thing we notice is that both generators, and thus the whole group, preserve the partition

$$\{\{1, 7\}, \{2, 8\}, \{3, 9\}, \{4, 10\}, \{5, 11\}, \{6, 12\}\}$$

This partition corresponds to the  $180^\circ$  rotational symmetry around the origin that the map exhibits, which is the map  $(X, Y) \mapsto (X, -Y)$  in the curve. If we map  $\{1, 2, 3, 4, 5, 6\} \leftrightarrow \{\{1, 7\}, \{2, 8\}, \{3, 9\}, \{4, 10\}, \{5, 11\}, \{6, 12\}\}$  in the obvious way, this induces a homomorphism  $\pi : \mathcal{C} \longrightarrow S_6$ , which takes

$$\begin{aligned} x = (1, 2, 3, 7, 8, 9)(6, 12) &\longmapsto (1, 2, 3) \\ y = (1, 4)(2, 5)(7, 10)(8, 11)(3, 6, 9, 12) &\longmapsto (1, 4)(2, 5)(3, 6) \end{aligned}$$

After few calculations, we see that the image of this map is the group

$$F = \langle x, y | x^3 = y^2 = [x, x^y] = 1 \rangle \cong \mathbb{Z}/2\mathbb{Z} \ltimes (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$$

Where the action of  $\mathbb{Z}/2\mathbb{Z}$  on  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  is given by interchanging the coordinates, and the map that takes  $\pi(\mathcal{C})$  to  $\mathbb{Z}/2\mathbb{Z} \ltimes (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$  takes  $\pi(x)$  to  $(0, 1, 0)$  and  $\pi(y)$  to  $(1, 0, 0)$ .  $\pi(x^y)$  is then  $(0, 0, 1)$ . The semidirect product  $\mathbb{Z}/2\mathbb{Z} \ltimes (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$  can also be seen as the wreath product  $\mathbb{Z}/3\mathbb{Z} \wr_{\{1,2\}} S_2$ .

The kernel of the map  $\pi$  is composed of the permutations that fix the previous partition pointwise, that is

$$\mathcal{C} \cap \langle (1, 7), (2, 8), (3, 9), (4, 10), (5, 11), (6, 12) \rangle$$

We will call the group  $\langle (1, 7), (2, 8), (3, 9), (4, 10), (5, 11), (6, 12) \rangle = \overline{K}$ , and its intersection with  $\mathcal{C}$  will be called  $K$ . Let us find out what  $K$  is. It is the kernel of the map  $\pi$ , so it is generated by the relations defining its image group. Thus, it is the normal subgroup of  $\mathcal{C}$  generated by  $\{x^3, y^2, [x, x^y]\}$ . To simplify the notation, we will call the transpositions in  $\overline{K}$   $a_i = (i, i+6)$ . Since the group they generate is commutative, we will use additive notation, so, for instance,  $a_1 + a_2$  means  $(1, 7)(2, 6)$ . Note that the group generated by the  $a_i$ 's is isomorphic to  $(\mathbb{Z}/2\mathbb{Z})^6$ . With this notation, we have

$$x^3 = a_1 + a_2 + a_3 + a_6; y^2 = a_3 + a_6; [x, x^y] = a_2 + a_3 + a_5 + a_6$$

All the generators lie in the subgroup  $\overline{K} \cap A_{12}$ . Let us produce a set of generators of this group within  $K$  to prove that  $K = \overline{K} \cap A_{12} \cong (\mathbb{Z}/2\mathbb{Z})^5$ . The set of generators can be given this way:

$$\begin{aligned} x^3 y^2 &= a_1 + a_2 & (x^3 y^2)^y &= a_4 + a_5 \\ (x^3 y^2)^x &= a_2 + a_3 & (x^3 y^2)^{xy} &= a_5 + a_6 \\ y^2 &= a_3 + a_6 \end{aligned}$$

So we conclude that the kernel of  $\pi$  is  $K = A_{12} \cap \overline{K}$ , which is isomorphic to  $(\mathbb{Z}/2\mathbb{Z})^5$ . Thus, the group  $\mathcal{C}$  is an extension of  $F \cong \mathbb{Z}/3\mathbb{Z} \wr S_2$  by the group  $(\mathbb{Z}/2\mathbb{Z})^5$ , and in particular its order is  $(3^2 \cdot 2) \cdot 2^5 = 2^6 \cdot 3^2$ . Since the normal subgroup is abelian,  $F$  is mapped into  $\text{Aut}(K)$ , and if we see  $K$  as a vector subspace of  $(\mathbb{Z}/2\mathbb{Z})^6$ , we can write the images of  $F$  in  $\text{Aut}(K)$  using matrices, like so:

$$x \mapsto \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}; y \mapsto \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$K$  is an  $F$ -module with the action induced by these matrices.

The subgroup of  $\widehat{F}_2$  corresponding to the dessin  $\widetilde{D}_0$  is the group of relations defining  $\mathcal{C}$ . For example, one such relation is  $x^3 y^2 (x^3 y^2)^x (x^3 y^2)^{x^2} = 1$ , since

$$x^3 y^2 (x^3 y^2)^x (x^3 y^2)^{x^2} = (a_1 + a_2) + (a_1 + a_2)^x + (a_1 + a_2)^{x^2} = a_1 + a_2 + a_2 + a_3 + a_3 + a_1 = 0$$

We will see that this relation is not satisfied by the dessins which are Galois conjugate to  $\widetilde{D}_0$ .

### 3.3 The dessins conjugate to $\widetilde{D}_0$

We will now look at the conjugate dessins to our original dessin  $(C, f)$  and its regular cover  $\widetilde{D}_0$ . Recall that the Galois action preserves regular covers (proposition 1.5.4), so the dessins conjugate to  $\widetilde{D}_0$  are the regular covers of the dessins conjugate to  $D_0$ . Therefore, if we take a  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  that maps our dessin  $(C, f)$  to some dessin  $(C^\sigma, f^\sigma)$ , it will map  $(C, f)$  to  $(C^\sigma, f^\sigma)$ . What we need then is to find the dessins conjugate to  $(C, f)$  and their regular covers.

Our dessin is defined over the field  $\mathbb{Q}(\sqrt[3]{2})$ , so its field of moduli is contained in this field, and to know its image by a Galois automorphism  $\sigma$ , it suffices to know  $\sigma(\sqrt[3]{2})$ . Therefore, there are two other dessins,  $D_1$  and  $D_2$ , conjugate to  $(C, f)$ , which are given by the Belyi pairs  $(C_1, f_1)$  and  $(C_2, f_2)$ , where

$$C_1 = V(Y^2 = X(X-1)(X-\xi\sqrt[3]{2})); C_2 = V(Y^2 = X(X-1)(X-\xi^2\sqrt[3]{2}))$$

The maps  $f_1$  and  $f_2$  have the same expression as  $f$ , namely  $(X, Y) \mapsto 1 - (X^3 - 1)^2$ , since it is defined over  $\mathbb{Q}$ . Note that these dessins are all different, since the underlying curves are not isomorphic. A different proof of this fact will follow from the fact that their regular covers are not isomorphic.

We will use the same procedure as before to draw the dessins. We start with the map  $X \mapsto 1 - (X^3 - 1)^2$ , as in figure 3.1, since this part of the map is the same for all three. Now, the last part is different, since for  $D_1$  it is ramified over  $\{0, 1, \xi\sqrt[3]{2}, \infty\}$  and for  $D_2$  over  $\{0, 1, \xi^2\sqrt[3]{2}, \infty\}$ . Like it happened before, the only face of the dessins will look the same as figure 3.2, since  $\infty$  is ramified. For  $D_1$ , the points  $\sqrt[3]{2}$  and  $\xi^2\sqrt[3]{2}$  are unramified, so we know the way their neighboring edges are identified. Once the neighboring sides to the points over  $\xi^2\sqrt[3]{2}$  are identified, we see the way the neighboring sides to  $\xi^2$  are identified. An analogous reasoning holds for  $D_2$ .

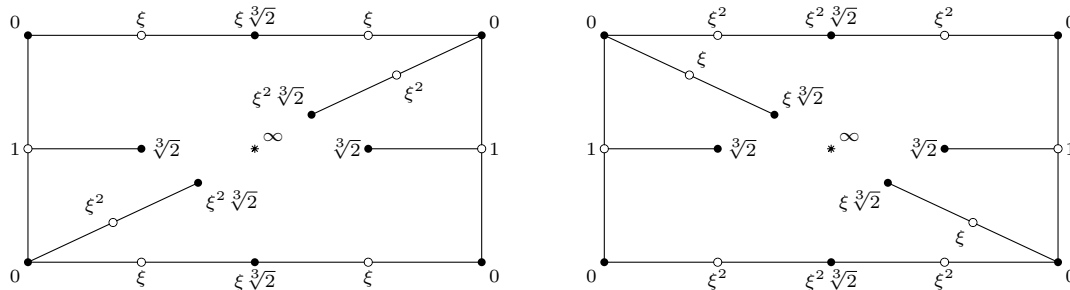
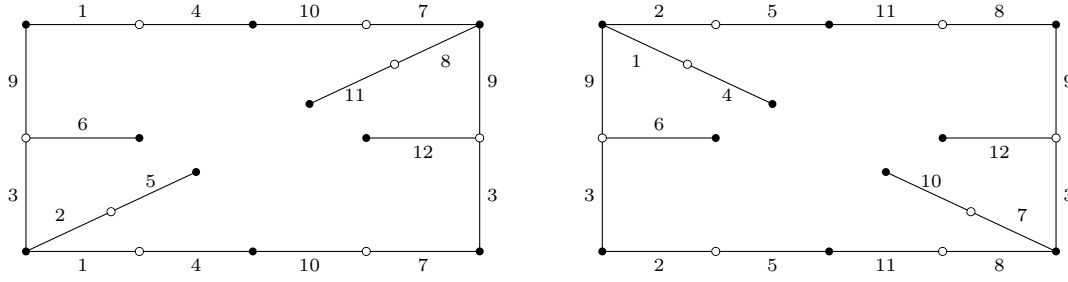


Figure 3.4: To the left, the points on  $C_1$  and to the right, the points on  $C_2$

In order to see how the remaining edges are identified, note that the edges surrounding 1 have just one way to be identified in order for 1 to be ramified, and the same thing happens with the edges surrounding  $\xi\sqrt[3]{2}$  (in  $C_1$ ). The four remaining edges then have only one way to be paired for 0 to have one preimage, and similarly for  $C_2$ . Thus, the opposing sides of the rectangle are identified. We can then number the edges as follows:

Figure 3.5: The way the edges are identified in  $C_1$  and  $C_2$ , with a numbering.

This way, the cartographic group of  $D_1$  can be seen as generated by  $x = (1, 2, 3, 7, 8, 9)(4, 10)$  and  $y = (1, 4)(2, 5)(7, 10)(8, 11)(3, 6, 9, 12)$ , and the cartographic group of  $D_2$  is generated by  $x = (1, 2, 3, 7, 8, 9)(5, 11)$  and  $y = (1, 4)(2, 5)(7, 10)(8, 11)(3, 6, 9, 12)$ . We will call the cartographic groups  $\mathcal{C}_1 = \widehat{F}_2/\widehat{D}_1$  and  $\mathcal{C}_2 = \widehat{F}_2/\widehat{D}_2$ . In terms of subgroups of  $\widehat{F}_2$ , this means that to the dessins  $D_1$  and  $D_2$  correspond two open subgroups such that the action of  $\widehat{F}_2$  on their right cosets gives these permutations.

Note that with the numbering we have chosen, the maps  $\pi_1 : \mathcal{C}_1 \rightarrow F < S_6$  and  $\pi_2$  can be defined the same as for  $\mathcal{C}$ , and that the images of  $x$  and  $y$  are still (123) and (14)(25)(36) respectively. The kernels are the same subgroups of  $S_{12}$  (isomorphic to  $\mathbb{Z}/2\mathbb{Z}^5$ ), and the kernels of  $\pi_1$  and  $\pi_2$  are isomorphic to the kernel of  $\pi$  as  $F$ -modules.

However, in  $\mathcal{C}_1$ ,  $x^3 = a_1 + a_2 + a_3 + a_4$ , so  $x^3y^2 = a_1 + a_2 + a_3 + a_4 + a_3 + a_6 = a_1 + a_2 + a_4 + a_6$ . This gives a hint that there may not be an isomorphism between the cartographic groups preserving  $x$  and  $y$ . Indeed, the relation  $x^3y^2(x^3y^2)^x(x^3y^2)^{x^2} = 1$ , which holds in  $\mathcal{C}$ , in  $\mathcal{C}_1$  reads

$$\begin{aligned} x^3y^2(x^3y^2)^x(x^3y^2)^{x^2} &= (a_1 + a_2 + a_4 + a_6) + (a_1 + a_2 + a_4 + a_6)^x + (a_1 + a_2 + a_4 + a_6)^{x^2} = \\ &= (a_1 + a_2 + a_4 + a_6) + (a_2 + a_3 + a_4 + a_6) + (a_3 + a_1 + a_4 + a_6) = a_4 + a_6 \neq 0 \end{aligned}$$

And analogously, in  $\mathcal{C}_2$ ,

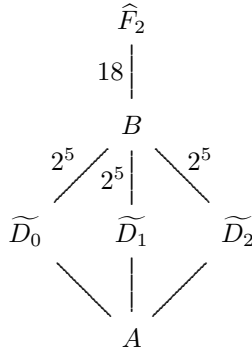
$$x^3y^2(x^3y^2)^x(x^3y^2)^{x^2} = a_5 + a_6$$

This means that there is no isomorphism from  $\mathcal{C}$  to  $\mathcal{C}_1$  (or  $\mathcal{C}_2$ ) taking  $x$  to  $x$  and  $y$  to  $y$ , since it wouldn't map  $x^3y^2(x^3y^2)^x(x^3y^2)^{x^2}$  to 1. If there is no isomorphism, the dessin  $\widetilde{D}_0$  is not fixed by the Galois action: take  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  such that  $\sigma(\sqrt[3]{2}) = \xi\sqrt[3]{2}$ . Then,  $D_0^\sigma = D_1$ , and  $(\widetilde{D}_0)^\sigma = \widetilde{D}_0^\sigma = \widetilde{D}_1$ . But  $\widetilde{D}_0$  and  $\widetilde{D}_1$  are not conjugate: since they are normal, if they were conjugate they would have to be the same group, but  $x^3y^2(x^3y^2)^x(x^3y^2)^{x^2}$  belongs to  $\widetilde{D}_0$  but not to  $\widetilde{D}_1$ . The same applies to a  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  taking  $\sqrt[3]{2}$  to  $\xi^2\sqrt[3]{2}$ : it would map  $\widetilde{D}_0$  to  $\widetilde{D}_2$ , and it is not the same group for the same reason.

We conclude that an automorphism  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  fixes  $\widetilde{D}_0$  if and only if it fixes  $\sqrt[3]{2}$ . This means that the field of moduli of  $\widetilde{D}_0$  is  $\mathbb{Q}(\sqrt[3]{2})$ . In particular, we have constructed a regular dessin with non-abelian field of moduli. For  $\widetilde{D}_1$  and  $\widetilde{D}_2$ , since they are conjugate to  $\widetilde{D}_0$ , we have that their fields of moduli are  $\mathbb{Q}(\xi\sqrt[3]{2})$  and  $\mathbb{Q}(\xi^2\sqrt[3]{2})$ , respectively.

We can calculate the genus  $g$  of  $\widetilde{D}_0$ : the monodromy action on it is given by the group acting on itself. Therefore, its edges are the elements of the group  $\mathcal{C}$ , it has a face for every 12 edges (since  $xy$  has order 12), a black vertex for every 6 edges (the order of  $x$ ), and a white vertex for every 4 edges. Its Euler-Poincaré characteristic is then  $2g - 2 = |\mathcal{C}| \left( \frac{1}{|x|} + \frac{1}{|y|} + \frac{1}{|xy|} - 1 \right) = 2^6 \cdot 3^2 \left( \frac{1}{6} + \frac{1}{4} + \frac{1}{12} - 1 \right) = 2^4 \cdot 3 \cdot 5 = 288$ . So its genus is 145.

We are going to make another interpretation of this picture in terms of subgroups of  $\widehat{F}_2$ , and to use it to give an example with smaller genus. We have three subgroups  $\widetilde{D}_0$ ,  $\widetilde{D}_1$  and  $\widetilde{D}_2$  of  $\widehat{F}_2$ , which are permuted by the action of the Galois group. Their intersection is then some subgroup  $A$  of  $\widehat{F}_2$ , and by its construction it must be fixed by the Galois action (and since it is a regular dessin, it is defined over its field of moduli, which is  $\mathbb{Q}$ ). The quotients  $\widehat{F}_2/\widetilde{D}_i$  are the cartographic groups of the dessins, and we have seen they can all be mapped into the group  $F$ . This means that the group  $B$  of defining relations for  $F$  contains all of them, and it is also fixed by the Galois action.



Let us find out what lies between  $A$  and  $B$ , specifically, about the group  $B/A$ . Note that, since  $B/\widetilde{D}_0$ ,  $B/\widetilde{D}_1$  and  $B/\widetilde{D}_2$  are commutative,  $B/(\widetilde{D}_0 \cap \widetilde{D}_1 \cap \widetilde{D}_2) = B/A$  also is commutative, and therefore  $\widehat{F}_2/B = F$  acts on it, so  $B/A$  is an  $F$ -module. In order to find out about its structure, we can use the  $F$ -module homomorphism

$$\begin{aligned}
J : \frac{B}{\widetilde{D}_0 \cap \widetilde{D}_1 \cap \widetilde{D}_2} &\longrightarrow \frac{B}{\widetilde{D}_0} \times \frac{B}{\widetilde{D}_1} \times \frac{B}{\widetilde{D}_2} \\
g &\longmapsto \left( g \bmod \widetilde{D}_0, g \bmod \widetilde{D}_1, g \bmod \widetilde{D}_2 \right)
\end{aligned}$$

This map is obviously well-defined and injective, and therefore its image is isomorphic to  $B/(\widetilde{D}_0 \cap \widetilde{D}_1 \cap \widetilde{D}_2)$ . We will call its image  $\overline{B} = J(B)$ , and as a module it is a submodule of  $K \times K \times K$  (recall the definition of  $K$ :  $K \cong B/\widetilde{D}_0 \cong B/\widetilde{D}_1 \cong B/\widetilde{D}_2 \cong \mathbb{Z}/2\mathbb{Z}^5$ ).

The  $F$  action on  $\overline{B}$  comes from the  $F$  action on each of the modules  $K$ , like so:  $J(g)^a = J(g^a) = (g^a \bmod \widetilde{D}_0, g^a \bmod \widetilde{D}_1, g^a \bmod \widetilde{D}_2)$ . Overall, we know the image of  $J$  is generated as an  $F$ -module by  $J(x^3)$ ,  $J(y^2)$  and  $J([x, x^y])$ , because  $x^3$ ,  $y^2$  and  $[x, x^y]$  generate  $B$  as an  $F$ -module. We can use this to compute the image. The map on the generators goes as follows:

$$\begin{aligned}
x^3 &\longmapsto (a_1 + a_2 + a_3 + a_6, \quad a_1 + a_2 + a_3 + a_4, \quad a_1 + a_2 + a_3 + a_5) \\
y^2 &\longmapsto (a_3 + a_6, \quad a_3 + a_6, \quad a_3 + a_6) \\
[x, x^y] &\longmapsto (a_2 + a_3 + a_5 + a_6, \quad a_1 + a_3 + a_4 + a_6, \quad a_1 + a_2 + a_4 + a_5)
\end{aligned}$$

We need to play around with the images for a bit to produce as many generators as we can. For example, using the image of  $y^2$ , we can generate every element of the form  $(a, a, a)$ , like so:

$$\begin{aligned}
y^2 &\longmapsto (a_3 + a_6, \quad a_3 + a_6, \quad a_3 + a_6) \\
y^2(y^2)^x &\longmapsto (a_1 + a_3, \quad a_1 + a_3, \quad a_1 + a_3) & (y^2)^y(y^2)^{xy} &\longmapsto (a_4 + a_6, \quad a_4 + a_6, \quad a_4 + a_6) \\
y^2(y^2)^{x^2} &\longmapsto (a_2 + a_3, \quad a_2 + a_3, \quad a_2 + a_3) & (y^2)^y(y^2)^{x^2y} &\longmapsto (a_5 + a_6, \quad a_5 + a_6, \quad a_5 + a_6)
\end{aligned} \tag{3.1}$$

Also, we can produce other elements, like

$$\begin{aligned}
x^3 y^2 &\longmapsto (a_1 + a_2, a_1 + a_2 + a_4 + a_6, a_1 + a_2 + a_5 + a_6) \\
\varphi = x^3 y^2 (y^2)^x (y^2)^{x^2} &\longmapsto (0, \quad a_4 + a_6, \quad a_5 + a_6) & \varphi^y &\longmapsto (0, \quad a_1 + a_3, \quad a_2 + a_3) \\
\varphi^{x^y} &\longmapsto (0, \quad a_4 + a_5, \quad a_4 + a_6) & \varphi^{yx} &\longmapsto (0, \quad a_1 + a_2, \quad a_1 + a_3)
\end{aligned} \tag{3.2}$$

We claim that the generators we have come up with so far generate the whole module as a group, i.e. if we define the submodule  $K'$  of  $K$  as  $K' = \{n_1 a_1 + n_2 a_2 + n_3 a_3 + n_4 a_4 + n_5 a_5 + n_6 a_6 \in K : n_1 + n_2 + n_3 \equiv n_4 + n_5 + n_6 \equiv 0 \bmod 2\}$ , it is clearly a codimension 1 submodule of  $K$ , that is, an index 2 subgroup, and we claim that the whole module  $M$  is given by

$$M = \{(a, a, a) : a \in K\} + \{(0, a', a'^{(xx^y)^{-1}}) : a \in K, a' \in K'\}$$

The proof goes as follows: first of all, this is indeed an  $F$ -module, since it is invariant under the actions of  $x$  and  $y$  (because  $(xx^y)^{-1}$  commutes with both  $x$  and  $y$ ), and second of all, the images of  $x^3$ ,  $y^2$  and  $[x, x^y]$ , which are the generators for the module, lie in  $M$ , since

$$\begin{aligned}
J(x^3) &= (a_1 + a_2 + a_3 + a_6, a_1 + a_2 + a_3 + a_4, a_1 + a_2 + a_3 + a_5) = \\
&= (a_1 + a_2 + a_3 + a_6, a_1 + a_2 + a_3 + a_6, a_1 + a_2 + a_3 + a_6) + (0, a_4 + a_6, a_5 + a_6) \\
J(y^2) &= (a_3 + a_6, a_3 + a_6, a_3 + a_6) \\
J([x, x^y]) &= (a_2 + a_3 + a_5 + a_6, a_1 + a_3 + a_4 + a_6, a_1 + a_2 + a_4 + a_5) = \\
&= (a_2 + a_3 + a_5 + a_6, a_2 + a_3 + a_5 + a_6, a_2 + a_3 + a_5 + a_6) + (0, a_1 + a_2 + a_4 + a_5, a_1 + a_3 + a_5 + a_6)
\end{aligned}$$

Also, we have already seen that the image of  $J$  generates at least the whole module we have given, since the generators for the first summand are given in (3.1) and the generators for the second are given in (3.2). Therefore,  $B/A \cong M$ .

The first module in the description of  $\overline{B}$  has dimension 5 as a  $\mathbb{Z}/2\mathbb{Z}$ -vector space, and the second module has dimension 4. The modules clearly intersect only at 0, so the sum is direct.

Let us give a nicer description of the module  $\overline{B}$ . If we let  $t = a_1 + a_2 + a_3 + a_4 + a_5 + a_6 \in K$ , we can write an element  $a \in K$  as  $a = a' + \varepsilon_a t$ , where  $a' \in K'$  and  $\varepsilon_a \in \{0, 1\}$ . Since an element of  $\overline{B}$  can be written as  $(a, a, a) + (0, a', a'^{(xx^y)^{-1}})$ , where  $a \in K$  and  $a' \in K'$ , we can decompose  $a$  to obtain

$$\begin{aligned} (a, a, a) + (0, k', k'^{(xx^y)^{-1}}) &= (a' + \varepsilon_a t, a' + \varepsilon_a t, a' + \varepsilon_a t) + (0, k', k'^{(xx^y)^{-1}}) = \\ &= \varepsilon_a(t, t, t) + (a', a', a') + (0, k', k'^{(xx^y)^{-1}}) \\ &= \varepsilon_a(t, t, t) + (a', 0, a'^{xx^y}) + (0, k' + a', k'^{(xx^y)^{-1}} + a' + a'^{xx^y}) \end{aligned}$$

Now, note that for all  $a' \in K'$ ,  $a + a^{xx^y} + a^{(xx^y)^{-1}} = 0$ , so  $a' + a'^{xx^y} = a'^{(aa^y)^{-1}}$ , and, if we call  $b' = k' + a'$ , this means that

$$(a, a, a) + (0, k', k'^{(xx^y)^{-1}}) = \varepsilon_a(t, t, t) + (a', 0, a'^{xx^y}) + (0, b', b'^{(xx^y)^{-1}})$$

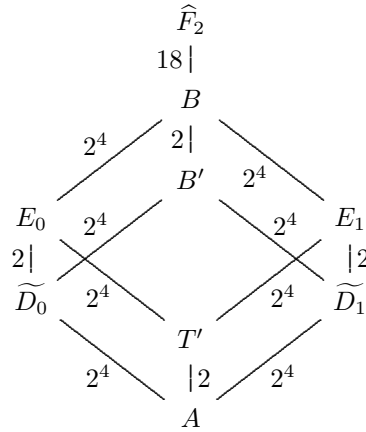
Thus,  $\overline{B}$  can be decomposed in the following way:

$$\overline{B} = \langle (t, t, t) \rangle \oplus \{(0, a, a^{(xx^y)^{-1}}) : a \in K\} \oplus \{(a, 0, a^{xx^y}) : a \in K\} = T \oplus \overline{K}_0 \oplus \overline{K}_1 \quad (3.3)$$

The sum is direct since one module doesn't intersect the sum of the other two. Note that the first module is isomorphic to  $\mathbb{Z}/2\mathbb{Z}$  with the trivial action and that the second and third modules are isomorphic to  $K$ . The order of  $M$  is then  $2 \cdot |K| \cdot |K| = 2^9$ .

Also, we can see what  $\widetilde{D}_0$  is mapped into in  $\overline{B}$ : its image is composed of the elements with first coordinate 0 (since this coordinate is  $g \bmod \widetilde{D}_0$ ), which is the submodule  $\overline{K}_0$ . Similarly,  $J(\widetilde{D}_1) = \overline{K}_1$ , and finally, the image of  $\widetilde{D}_2$  is the elements of third coordinate 0, which is the module  $\overline{K}_2 = \{(a^{(xx^y)^{-1}}, a^{xx^y}, 0) : a \in K\}$ . It follows that  $(\widetilde{D}_0 \cap \widetilde{D}_1)/(\widetilde{D}_0 \cap \widetilde{D}_1 \cap \widetilde{D}_2) \cong \overline{K}_0 \cap \overline{K}_1 = 0$ , so  $\widetilde{D}_0 \cap \widetilde{D}_1 = \widetilde{D}_0 \cap \widetilde{D}_1 \cap \widetilde{D}_2$ .

We can now draw a diagram of the subgroups of  $\widehat{F}_2$  with more information: If we call  $B' = \widetilde{D}_0 \widetilde{D}_1$  (that is,  $B' = J^{-1}(\overline{K}_0 + \overline{K}_1)$ ),  $E_i = J^{-1}(K_i + T)$ , and  $T' = J^{-1}(T)$ , we can draw the following:



We are omitting  $\widetilde{D}_2$  and  $E_2$  for simplicity. There are three groups, namely  $E_0$ ,  $E_1$  and  $E_2$ , which contain the dessins we are working with, the  $\widetilde{D}_i$ 's, and since the Galois group preserves the subgroup structure, they can't be left fixed by its action. In the next section, we will see that the Galois group has the same action on these dessins, which have smaller genus, namely 61 (which we will see), and smaller degree, namely  $18 \cdot 2^4 = 288$ .

### 3.4 Another dessin with non-abelian field of moduli

In the previous diagram, there was a group  $E_i$  containing each of the  $\widetilde{D}_i$ . Let us see that if  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  sends  $\widetilde{D}_i$  to  $\widetilde{D}_j$ , then  $E_i^\sigma = E_j$  also. In order to do this, we are going to see that  $E_i/\widetilde{D}_i$  is the center of  $\widehat{F}_2/\widetilde{D}_i = \mathcal{C}_i$ .

First of all, the center of  $\widehat{F}_2/\widetilde{D}_i$  has to be contained in the projection of the center of  $\widehat{F}_2/B$ , which is  $\{1, xx^y, (xx^y)^2\}$ . However,  $xx^y$  doesn't act trivially on the module, so its class is not in the center. Therefore,

$Z(\widehat{F}_2/\widetilde{D}_i) \subset B/\widetilde{D}_i \cong T \oplus K$ , and it must be the set of elements fixed by the  $F$ -action. It is straightforward to see that the elements fixed by the  $F$  action are the elements of  $T = T'/A = \{0, (t, t, t)\}$ .

Therefore, the modules  $E_i$  are the centers of  $\widehat{F}_2/\widetilde{D}_i$ , and they are characteristic subgroups of them. Since the Galois group acts by automorphisms of  $\widehat{F}_2$ , if  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  takes  $\widetilde{D}_i$  to  $\widetilde{D}_j$ , it will induce an isomorphism of the quotients  $\widehat{F}_2/\widetilde{D}_i$  and  $\widehat{F}_2/\widetilde{D}_j$ , which will map  $Z(\widehat{F}_2/\widetilde{D}_i) = E_i$  to  $Z(\widehat{F}_2/\widetilde{D}_j) = E_j$ . Therefore, the action of the Galois group on the  $E_i$ 's is the same as the action on the  $\widetilde{D}_i$ 's, and in particular the field of moduli of  $E_i$  is  $\mathbb{Q}(\xi^i \sqrt[3]{2})$ .

If we look at  $E_i/\widetilde{D}_i$  as a subgroup of  $\widehat{F}_2/\widetilde{D}_i$ , it is a subgroup of order 2, and it is generated by  $J^{-1}(t, t, t) \bmod \widetilde{D}_i = a_1 + a_2 + a_3 + a_4 + a_5 + a_6$ . As permutations,  $E_i/\widetilde{D}_i = \{1, (1, 7)(2, 8)(3, 9)(4, 10)(5, 11)(6, 12)\} < \mathcal{C}_i$ . Therefore,

$$\frac{\widehat{F}_2}{E_i} \cong \frac{\mathcal{C}_i}{E_i/\widetilde{D}_i} = \frac{\mathcal{C}_i}{\langle (1, 7)(2, 8)(3, 9)(4, 10)(5, 11)(6, 12) \rangle}$$

Note that  $(xy)^6 = (1, 7)(2, 8)(3, 9)(4, 10)(5, 11)(6, 12)$ , so in the cartographic group of this dessin,  $z$  will have order 6. Since the orders of  $x$  and  $y$  are 6 and 4 respectively, the formula for the Euler-Poincaré characteristic is  $2 - 2g = 24 \cdot 12 \cdot (\frac{1}{6} + \frac{1}{4} + \frac{1}{6} - 1) = -120$ , so the genus is 61.

Now, the module  $T' = E_0 \cap E_1 \cap E_2$  is fixed by the Galois action, and the quotient  $B/T'$  is isomorphic to  $K_0 \oplus K_1$ , since we are taking the quotient by the module  $T$ . The module  $E_0/T$ , for instance, maps into  $(T \oplus K_0)/T \cong K_0$ .

We can represent the module  $K'$  by means of the finite field with four elements  $\mathbb{F}_4$ . If we see it as  $\mathbb{F}_4 = \mathbb{F}_2[\xi]$  for a cubic root of unity  $\xi$ , we can take the group isomorphism

$$\begin{aligned} \Phi : K' &\longrightarrow \mathbb{F}_4^2 \\ a_1 + a_2 &\longmapsto (1, 0) \\ a_2 + a_3 &\longmapsto (\xi^2, 0) \\ a_4 + a_5 &\longmapsto (0, 1) \\ a_5 + a_6 &\longmapsto (0, \xi^2) \end{aligned}$$

And the homomorphism

$$\begin{aligned} \rho : F &\longrightarrow GL_2(\mathbb{F}_4) \\ x &\longmapsto \begin{pmatrix} \xi^2 & 0 \\ 0 & 1 \end{pmatrix} \\ y &\longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

The reason we are taking  $\xi^2$  and not  $\xi$  is that in the next section, notation will be easier to remember. One can check that  $\Phi(a)\rho(g) = \Phi(a^g)$ , so we have a nice module isomorphic to  $K'$ . Since  $B/T' \cong K' \times K'$ , we have another description of the module  $B/T'$ . Also, its generators are given by

$$\begin{array}{llllll} x^3 & \xrightarrow[\Phi \times \Phi]{J} & (a_1 + a_2 + a_3 + a_6, a_1 + a_2 + a_3 + a_4, \cdot) & \stackrel{\text{mod } T'}{\equiv} & (a_4 + a_5, a_5 + a_6) & \xrightarrow{\Phi \times \Phi} \\ & & (0, 1, 0, \xi^2) & & & \\ y^2 & \xrightarrow[\Phi \times \Phi]{J} & (a_3 + a_6, a_3 + a_6, \cdot) & \stackrel{\text{mod } T'}{\equiv} & (a_1 + a_2 + a_4 + a_5, a_1 + a_2 + a_4 + a_5) & \xrightarrow{\Phi \times \Phi} \\ & & (1, 1, 1, 1) & & & \\ [x, x^y] & \xrightarrow[\Phi \times \Phi]{J} & (a_2 + a_3 + a_5 + a_6, a_1 + a_3 + a_4 + a_6, \cdot) & \stackrel{\text{mod } T'}{\equiv} & (a_2 + a_3 + a_5 + a_6, a_1 + a_3 + a_4 + a_6, \cdot) & \xrightarrow{\Phi \times \Phi} \\ & & (\xi^2, \xi^2, \xi, \xi) & & & \end{array}$$

We are now going to give a more explicit description of the dessins  $E_i$ , with equations. We are going to give more explicit constructions of the dessin  $B$  and then describe  $E_0$  as a covering of this curve.

So let us look at the dessin  $B$ , which is a regular dessin with cartographic group  $F$ . If we look back on the dessins we used to construct the dessin  $D_0$ , we had that  $D_0$  was a two sheet covering of the dessin to the left in figure 3.1, by a map that we will call  $\pi$ . This means that the regular cover of that dessin is itself covered by the regular cover of  $D_0$ , which suggests that it might be the group  $B$ . As a matter of fact it is, for if we look at the permutations induced by  $x, y$ , they are precisely, given the right numbering of the edges,  $(1, 2, 3)$  and  $(1, 4)(2, 5)(3, 6)$ . This means that the dessin we are looking for is the regular cover of this dessin. In  $B$ ,  $x$  has order 3,  $y$  has order 2, and  $xy$  has order 6. This means two things: first, that  $B$  has genus 1, for  $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$ , and also the only points that are ramified are  $\{\sqrt[3]{2}, \xi \sqrt[3]{2}, \xi^2 \sqrt[3]{2}\}$ . This suggests taking the function  $(X - \sqrt[3]{2})(X - \xi \sqrt[3]{2})(X - \xi^2 \sqrt[3]{2}) = X^3 - 2$  which has order 1 at each of these points, and considering

the Fermat curve  $X^3 + Y^3 = 2$ , with the map  $(X, Y) \mapsto X$ . This map has degree 3 and it is only ramified over these three points (note that the point at infinity,  $(1 : 0)$ , has three preimages, namely  $(1 : 1 : 0)$ ,  $(1 : \xi : 0)$  and  $(1 : \xi^2 : 0)$ , so it is unramified).

We have the Belyi pair, which we will also call  $B$ , given by

$$(\{(X : Y : Z) \in \mathbb{P}^2 : X^3 + Y^3 = 2Z^3\}, (X : Y : Z) \mapsto Z^6 - (Z^3 - X^3)^2)$$

We can see that this map is regular: the Fermat curve has two automorphisms, namely  $(x, y) \mapsto (\xi x, y)$ , and  $(x, y) \mapsto (y, x)$ , both of which preserve the Belyi map (since  $1 - x^3 = y^3 - 1$ ), and they generate the group  $F$ . Since the degree of the pair is 18, and we have 18 automorphisms, it is the whole automorphism group, and the dessin is regular. This means that it is indeed the regular cover of the dessin in figure 3.1, and it corresponds to the group  $B$ , as we desired.

Our objective now is to draw the dessin  $B$ . It is easy to do, since we know its cartographic group, which is  $F$ , and its edges can be mapped to the cosets of  $B$ . If we see  $\widehat{F}_2/B$  as a subgroup of  $S_6$  (via the map  $x \mapsto (1, 2, 3)$  and  $y \mapsto (1, 4)(2, 5)(3, 6)$ ), we can draw the dessin, as it is seen in figure 3.6.

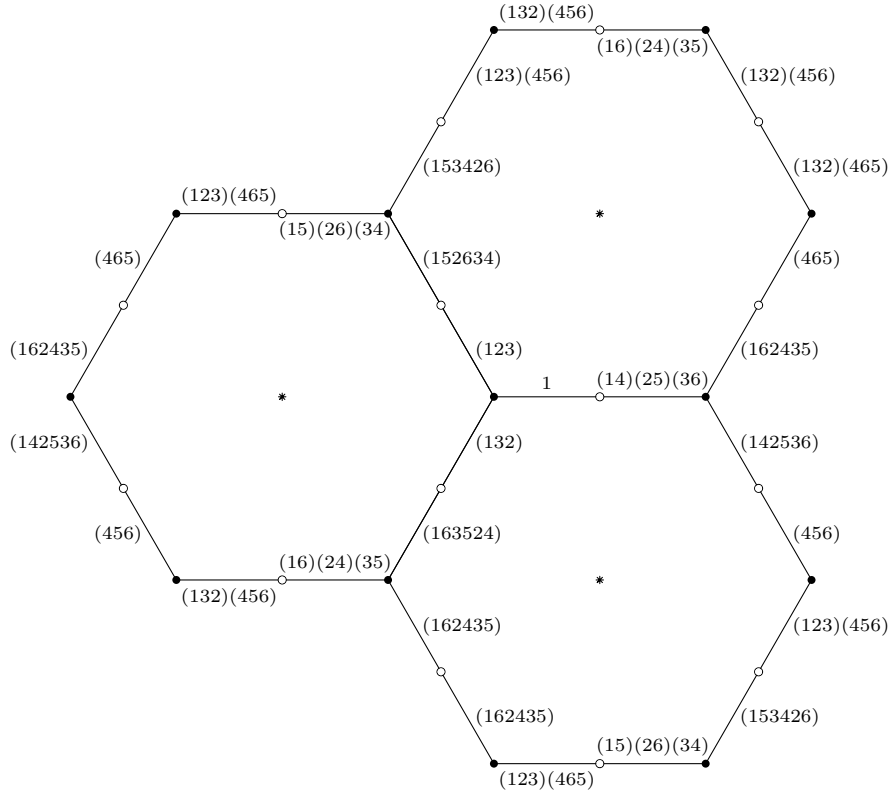


Figure 3.6: The dessin given by the group  $B$ , where the elements of  $\widehat{F}_2/B$  are seen as permutations.

In the preimage of  $\{0, 1, \infty\}$ , there are 18 points, namely

$$\begin{array}{lll} (0, \sqrt[3]{2}) & (1, 1) & (1 : -1 : 0) \\ (0, \xi \sqrt[3]{2}) & (1, \xi) & (1 : -\xi : 0) \\ (0, \xi^2 \sqrt[3]{2}) & (1, \xi^2) & (1 : -\xi^2 : 0) \\ (\sqrt[3]{2}, 0) & (\xi, 1) & \\ (\xi \sqrt[3]{2}, 0) & (\xi, \xi) & \\ (\xi^2 \sqrt[3]{2}, 0) & (\xi, \xi^2) & \\ & (\xi^2, 1) & \\ & (\xi^2, \xi) & \\ & (\xi^2, \xi^2) & \end{array}$$

Let us see how these points are distributed in the dessin: To do this, we can use its automorphism group, since we know it is  $F = \langle x, y : y^2 = x^3 = [x, x^y] = 1 \rangle$ , but on the other hand, the generator  $x$  can be seen as the map



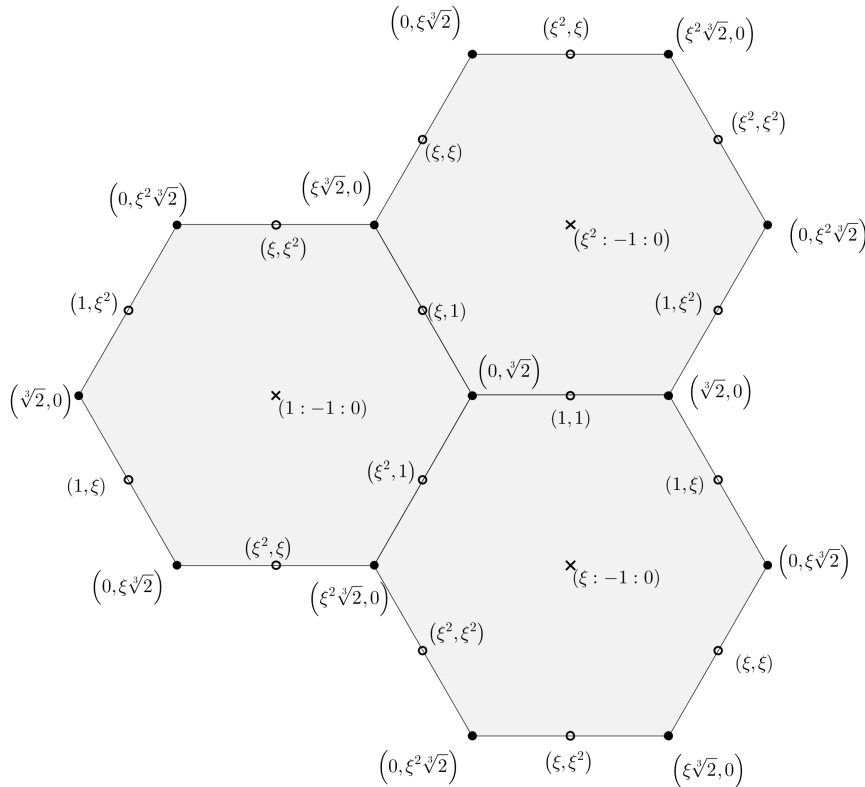


Figure 3.7: The points on the dessin  $B$

$(X, Y) \longmapsto (\xi X, Y)$ , and  $y$  can be seen as the map  $(X, Y) \longmapsto (Y, X)$ . Then, the map  $\pi$  is the quotient by the action of  $x^y$ , which is  $(X, Y) \longmapsto (X, \xi Y)$ .

In order to find out how the branch points are placed on the curve, we can use the action of the automorphism group on the dessin, which, since the dessin is regular, is the cartographic group acting on the left. Therefore, we can use figure 3.6 to see what the action is. Since the action is transitive on the edges and on vertices of the same color, we can choose any edge to contain the base point. We have chosen it to be the edge connecting  $(0, \sqrt[3]{2})$  and  $(1, 1)$  (which is indeed contained in the preimage of  $[0, 1]$ , since  $\pi(\{(t, \sqrt[3]{2-t^3}) : t \in [0, 1]\}) = [0, 1]$ ). If we place the points  $(0, \sqrt[3]{2})$  and  $(1, 1)$  on the base edge, the automorphism group, seen as  $x(X, Y) = (\xi X, Y); y(X, Y) = (Y, X)$ , gives the placement of the rest of the points, as seen in figure 3.7. (Note that, in figure 3.6, the action of  $x = (123)$  is given by  $120^\circ$  rotation around the middle point and the action of  $y = (14)(25)(36)$  is given by  $180^\circ$  rotation around the white point to the right of the middle point).

Using the dessin  $B$ , we are going to give equations for the dessin  $E_0$ , which is a covering of  $B$  of  $2^4$  sheets. We are going to construct a dessin of degree two over  $B$ , and the regular dessin that covers it will be the dessin  $E_0$ . To produce one of these dessins, we just need an index 2 subgroup of  $B$  containing  $E_0$ . Since  $B/E_0 \cong K \cong \mathbb{F}_4^2$ , we can take the subgroup  $H_0$  of this quotient given by  $\{(a, b) \in \mathbb{F}_4^2 : b \in \mathbb{F}_2\}$ , which is an index 2 subgroup. To this subgroup corresponds a dessin, which can be constructed as a covering of  $B$ . To do this, we will use that an index 2 subgroup of  $B$  (which is a free group on 19 generators, since it is the fundamental group of a curve of genus 1 with 18 points removed) can be determined by which of its generators are in the subgroup. It is straightforward to give, for a point on the Fermat curve, a loop going around it in  $\widehat{F}_2$ , and we can compute its image in  $K$ , since we did this in the previous section. Recall that  $x^3$  in  $B/E_0 \cap E_1$  maps to  $(a_4 + a_5, a_5 + a_6)$ , which modulo  $E_0$  is  $a_4 + a_5$ , and the isomorphism we gave maps this to  $(0, 1)$ . Similarly,  $y^2$  maps to  $(a_1 + a_2 + a_4 + a_5, a_1 + a_2 + a_4 + a_5)$ , and to  $(1, 1)$ . Also, we need the image of  $(xy)^6$ : in the cartographic groups  $\mathcal{C}_0$ ,  $\mathcal{C}_1$  and  $\mathcal{C}_2$ , its image is  $a_1 + a_2 + a_3 + a_4 + a_5 + a_6$ , so it is in the center, and it is contained in

$E_0 \cap E_1 \cap E_2$ . The result is the following:

Point	Generator	Image in $\mathbb{F}_4^2$	Point	Generator	Image in $\mathbb{F}_4^2$
$(0, \sqrt[3]{2})$	$x^3$	$(0, 1)$	$(1, 1)$	$y^2$	$(1, 1)$
$(0, \xi \sqrt[3]{2})$	$(x^3)^{(x^y)^2}$	$(0, \xi)$	$(\xi, 1)$	$(y^2)^{x^2}$	$(\xi, 1)$
$(0, \xi^2 \sqrt[3]{2})$	$(x^3)^{x^y}$	$(0, \xi^2)$	$(\xi^2, 1)$	$(y^2)^x$	$(\xi^2, 1)$
$(\sqrt[3]{2}, 0)$	$(x^3)^y$	$(1, 0)$	$(1, \xi)$	$(y^2)^{x^2 y}$	$(1, \xi)$
$(\xi \sqrt[3]{2}, 0)$	$(x^3)^{yx^2}$	$(\xi, 0)$	$(\xi, \xi)$	$(y^2)^{x^2 y x^2}$	$(\xi, \xi)$
$(\xi^2 \sqrt[3]{2}, 0)$	$(x^3)^{yx}$	$(\xi^2, 0)$	$(\xi^2, \xi)$	$(y^2)^{x^2 y x}$	$(\xi^2, \xi)$
$(1 : -1 : 0)$	$(xy)^6$	$(0, 0)$	$(1, \xi^2)$	$(y^2)^{xy}$	$(1, \xi^2)$
$(\xi : -1 : 0)$	$((xy)^6)^{x^2}$	$(0, 0)$	$(\xi, \xi^2)$	$(y^2)^{xy x^2}$	$(\xi, \xi^2)$
$(\xi^2 : -1 : 0)$	$((xy)^6)^x$	$(0, 0)$	$(\xi^2, \xi^2)$	$(y^2)^{xy x}$	$(\xi^2, \xi^2)$
—	$y^{-1} x^{-1} y x y x y x^{-1}$	$(1, 1)$	—	$y^{-1} x^{-1} y^{-1} x^{-1} y^{-1} x y x$	$(\xi^2, 1)$

The last two generators correspond to loops generating the fundamental group of the torus, and they are mapped in the permutation groups to  $(a_3 + a_6, a_1 + a_2 + a_3 + a_5, a_1 + a_4 + a_5 + a_6)$  and  $(a_1 + a_6, a_1 + a_2 + a_3 + a_5, a_2 + a_4 + a_5 + a_6)$ , which correspond to  $(1, 1, 0, \xi)$  and  $(\xi^2, 1, 0, \xi)$ . The generators which are not in the subgroup  $H$  are then  $\{(0, \xi \sqrt[3]{2}), (0, \xi^2 \sqrt[3]{2}), (1, \xi), (\xi, \xi), (\xi^2, \xi), (1, \xi^2), (\xi, \xi^2), (\xi^2, \xi^2)\}$ .

Let us look at the dessin's fields of functions.  $B$  has  $\overline{\mathbb{Q}}(B) = \overline{\mathbb{Q}}(X)[Y]/(X^3 + Y^3 - 2)$  as field of functions (and as a dessin, it is the extension  $\overline{\mathbb{Q}}(t = 1 - (1 - X^3)^2) \subset \overline{\mathbb{Q}}(B)$ ). The field of functions of the dessin  $H$  is an extension of degree 2 of  $\overline{\mathbb{Q}}(B)$ , and it will therefore be generated by an element  $Z$ , such that  $Z^2 \in \overline{\mathbb{Q}}(B)$ .

Now, we need to use the information we have on the ramification points of the map from the degree two covering of  $B$ , which we will call  $B_0$  to find out which is the element  $Z$  that generates the extension. Let us call  $\varphi = Z^2 \in \overline{\mathbb{Q}}(B)$ .

**Lemma 3.4.1.** *Let  $\overline{\mathbb{Q}}(B)$  be the field of functions of a curve  $B$ , and let  $\overline{\mathbb{Q}}(B_0) = \overline{\mathbb{Q}}(B)(Z)$  be the field of functions of a curve  $B_0$  such that  $Z^2 = \varphi \in \overline{\mathbb{Q}}(B)$ . Let  $\pi : B_0 \rightarrow B$  be the covering map. Then,  $\pi$  ramifies over a point  $P$  if and only if  $\text{ord}_P(\varphi)$  is odd.*

*Proof.* Suppose  $\text{ord}_P(\varphi)$  is odd. Multiplying by the square of a uniformizing parameter for  $P$ , we can assume that  $\text{ord}_P(\varphi) = 1$ . Now, if  $\nu$  is a valuation extending  $\text{ord}_P$  to  $\overline{\mathbb{Q}}(B_0)$ , then we must have that  $2\nu(Z) = \nu(Z^2) = \nu(\varphi)$ . Since  $\nu(\varphi)$  must be positive, it must equal at least 2. But, since the degree of the map is 2, there must be only one extension of the valuation, with ramification index 2.

Now, if  $\text{ord}_P(\varphi)$  is even, we can assume that it is 0, doing the same as in the previous case. For a valuation  $\nu$  extending  $\text{ord}_P(\varphi)$ , we must have  $\nu(Z) = 0$ . Now, let  $\pi$  be a uniformizing parameter for  $\text{ord}_P$ . Let  $\varphi(P) = a^2$ , and let  $\mathcal{O}_P$  be the local ring for  $P$ . Then,  $\mathcal{O}_P[Z]$  is a ring extending  $\mathcal{O}_P$  and it has two maximal ideals, namely  $(Z - a, \pi)$  and  $(Z + a, \pi)$ . Therefore, the valuation  $\text{ord}_P$  extends in at least two different ways, and since the maximum number of extensions it can have is 2, we must have that there are two of them, each unramified.  $\square$

So, we have that the covering is of the form  $\overline{\mathbb{Q}}(B) \subset \overline{\mathbb{Q}}(B)[Z]$ , where  $Z^2 = \varphi \in \overline{\mathbb{Q}}(B)$ . For the map to ramify at the list of points we want it to ramify,  $\varphi$  must have odd order at precisely the points  $\{(0, \xi \sqrt[3]{2}), (0, \xi^2 \sqrt[3]{2}), (1, \xi), (\xi, \xi), (\xi^2, \xi), (1, \xi^2), (\xi, \xi^2), (\xi^2, \xi^2)\}$ . One such function is

$$\varphi = \frac{(Y - \xi)(Y - \xi^2)}{(Y - \xi \sqrt[3]{2})(Y - \xi^2 \sqrt[3]{2})}$$

The problem is, this is not the only function with this property, not even modulo multiplication by squares. If we take the functions

$$\psi_1 = \frac{X + Y - 2}{X + Y - 2\xi}; \psi_2 = \frac{X + Y - 2\xi}{X + Y - 2\xi^2}; \psi_3 = \psi_2/\psi_1 = \frac{X + Y - 2\xi}{X + Y - 2\xi^2}$$

We have that their divisors of zeroes and poles are the following:

$$(\psi_1) = 2(1, 1) - 2(\xi, \xi); (\psi_2) = 2(1, 1) - 2(\xi^2, \xi^2); (\psi_3) = 2(\xi, \xi) - 2(\xi^2, \xi^2)$$

Since their order at every point is even, but they are not squares (because they would have to be squares of functions of degree 1, and there are no such functions on an elliptic curve), the functions  $\varphi\psi_i$  are also functions with odd order at the prescribed points, which are different from  $\varphi$  and from each other modulo squares. Let us prove that these are the only functions with even multiplicity at every point, modulo squares.

Suppose a function  $\psi$  has divisor of zeros and poles  $\sum 2n_i P_i$ . If we denote the sum in the elliptic curve by  $\oplus$ , we know that this means that  $\bigoplus 2n_i P_i = 0$  (see, for example, [15]). Now, if  $\psi$  is not a square, this means

that  $\bigoplus n_i P_i \neq 0$ , otherwise  $\bigoplus n_i P_i$  would be a principal divisor and a function with such divisor would be the square root of  $\psi$  except for a multiplicative constant. Therefore,  $\bigoplus n_i P_i$  is a point of order 2, of which there are three. Now, if we take  $(0, \sqrt[3]{2})$  as the origin for our curve, we have that the divisors of the  $\psi_i$ 's halved are all different in the group of the curve, since  $(1, 1) - (\xi, \xi) = (\xi \sqrt[3]{4}, -\sqrt[3]{2})$ ,  $(1, 1) - (\xi^2, \xi^2) = (\xi^2 \sqrt[3]{4}, -\sqrt[3]{2})$  and  $(\xi, \xi) - (\xi^2, \xi^2) = (\sqrt[3]{4}, -\sqrt[3]{2})$ . Therefore, we have that  $\bigoplus n_i P_i = \frac{1}{2}(\psi_j)$ , for some  $j$ . From this follows that  $\psi \psi_j^{-1}$  is a square, since it is the square of a function with divisor  $\bigoplus n_i P_i - \frac{1}{2}(\psi_j)$ , which is 0 in the Picard group, and therefore it is a principal divisor.

Thus we are left with 4 possibilities for the function we are looking for. Let us take a look at two modules. The first one is  $B/B^2$  (where  $B^2 = \langle g^2 : g \in B \rangle$ ). Since  $B$  is freely generated by 18 elements,  $B/B^2 \cong (\mathbb{Z}/2\mathbb{Z})^{18}$ .  $B^2$  is a characteristic subgroup of  $B$ , and therefore it is fixed by every automorphism of  $B$ , for example, by conjugation by an element of  $\hat{F}_2$ . Furthermore, since  $B/B^2$  is commutative, every element of  $B$  acts as the identity on the quotient  $B/B^2$ , so it is an  $\hat{F}_2/B$ -module, or an  $F$ -module.

The other module consists of the functions  $f \in \overline{\mathbb{Q}}(B)^\times$  such that  $\overline{\mathbb{Q}}(B)[\sqrt{f}]/\overline{\mathbb{Q}}(B)$  is ramified over at most the 18 points on the dessin. We take these functions with the product as a group law, and we quotient out by  $(\overline{\mathbb{Q}}(B))^2$ , so  $f \sim f'$  if and only if  $\overline{\mathbb{Q}}(B)[\sqrt{f}]$  and  $\overline{\mathbb{Q}}(B)[\sqrt{f'}]$  are the same fields of functions. This group, which we will call  $R$  obviously has exponent 2. Now, we can see that  $B/B^2$  and  $R$  are dual to one another.

If we take the field  $\mathcal{K}/\overline{\mathbb{Q}}(t)$ , which is the biggest extension unramified outside of  $\{0, 1, \infty\}$ , we can see  $B$  as  $\text{Gal}(\mathcal{K}/\overline{\mathbb{Q}}(B))$ . Now,  $B^2$  is the intersection of all the index 2 subgroups of  $B$ , and therefore the field of functions of the dessin corresponding to the group  $B^2$  will be the field  $\overline{\mathbb{Q}}(B^2)$  which is the field generated by all the field extensions of  $\overline{\mathbb{Q}}(B)$  of degree 2 unramified outside of  $\{0, 1, \infty\}$ .

Now, if we take an element  $g \in B/B^2 = \text{Gal}(\overline{\mathbb{Q}}(B^2)/\overline{\mathbb{Q}}(B))$ , and a function class  $f \in R$ , we can define a pairing with image  $\{\pm 1\}$  in the following way: choose a square root  $h$  of  $f$ , which generates a degree 2 extension of  $\overline{\mathbb{Q}}(B)$  unramified outside of the 18 points, and therefore contained in  $\overline{\mathbb{Q}}(B^2)$ . If  $h^g = h$ , then define  $\langle f, g \rangle = 1$ , and if  $h^g = -h$ , define  $\langle f, g \rangle = -1$ . In other words,  $\langle f, g \rangle = \frac{h^g}{h}$ . It is clear that this definition does not depend upon the choice of the square root, since  $(-h)^g = -h^g$ . Also, the pairing is bilinear: if one takes two functions  $f_1$  and  $f_2$  with square roots  $h_1$  and  $h_2$ , respectively, then  $\langle f_1 f_2, g \rangle = \frac{(h_1 h_2)^g}{h_1 h_2} = \frac{h_1^g}{h_1} \frac{h_2^g}{h_2} = \langle f_1, g \rangle \langle f_2, g \rangle$ , and if one takes two automorphisms  $g_1$  and  $g_2$ , then

$$\langle f, g_1 g_2 \rangle = \frac{h^{g_1 g_2}}{h} = \frac{h^{g_1 g_2}}{h^{g_2}} \frac{h^{g_2}}{h} = \left( \frac{h^{g_1}}{h} \right)^{g_2} \frac{h^{g_2}}{h} = \langle f, g_1 \rangle \langle f, g_2 \rangle$$

Because  $\langle f, g_1 \rangle$  is fixed by  $g$ . Finally, since the square roots of these functions generate the field  $\overline{\mathbb{Q}}(B^2)$ ,  $\langle f, g \rangle = 1$  for all  $f \in R$  implies that  $g \in B^2$ , and dually, if the square root of a function is fixed by every element of  $\text{Gal}(\overline{\mathbb{Q}}(B^2)/\overline{\mathbb{Q}}(B))$ , then it must lie in  $\overline{\mathbb{Q}}(B)$ , and the function is a square. Overall, the pairing is perfect, which means that  $R$  and  $B/B^2$  are dual as  $\frac{\mathbb{Z}}{2\mathbb{Z}}$ -vector spaces. In particular,  $R \cong (\mathbb{Z}/2\mathbb{Z})^{18}$ .

Now, let us look at the  $F$ -module structure:  $B/B^2$  is a left  $F$ -module with the action by conjugation and  $R$  is a left  $F$ -module with the action of  $F = \text{Gal}(\overline{\mathbb{Q}}(B)/\overline{\mathbb{Q}}(t))$ . Now, let  $\sigma \in F$ ,  $f \in R$ ,  $g \in B/B^2$ . If  $h$  is a square root of  $f$ , then, for any  $\tilde{\sigma} \in \hat{F}_2$  such that its class in  $\hat{F}_2/B = F$  is  $\sigma$ ,  $\tilde{\sigma}(h)$  will be a square root of  $f^{\tilde{\sigma}} = f^\sigma$ . Therefore,

$$\langle f^\sigma, g \rangle = \frac{h^{\tilde{\sigma}g}}{h^{\tilde{\sigma}}}$$

Now, since the right hand side equals  $\pm 1$ , it is fixed by  $\tilde{\sigma}^{-1}$ , so

$$\langle f^\sigma, g \rangle = \left( \frac{h^{\tilde{\sigma}g}}{h^{\tilde{\sigma}}} \right)^{\tilde{\sigma}^{-1}} = \frac{h^{g^{\tilde{\sigma}^{-1}}}}{h} = \langle f, g^{\sigma^{-1}} \rangle$$

Now, from this fact we can obtain a lot of information from the submodule structure of the modules: Since they are dual, to each subspace  $S < B/B^2$  we can associate to it its dual subspace  $S^* = \{g \in G : \langle S, g \rangle = 1\}$ , and vice versa. This correspondence is inclusion-reversing and it satisfies the identity  $S^{**} = S$ , and it is also the Galois correspondence: to a subspace  $S < R$  we associate the subgroup that fixes  $\overline{\mathbb{Q}}(B)[\{\sqrt{f} : f \in S\}]$ .

Now, if we take a subspace  $S < B/B^2$ , and an element  $\sigma \in F$ , we will have, from the previous identity, that  $(S^\sigma)^* = (S^*)^\sigma$ . If we denote by  $\bar{S}$  the module generated by  $S$ , and  $\dot{S}$  to be the largest submodule inside  $S$ , we will have

$$(\bar{S})^* = \left( \sum_{\sigma \in F} S^\sigma \right)^* = \bigcap_{\sigma \in F} (S^\sigma)^* = \bigcap_{\sigma \in F} (S^*)^\sigma = (\dot{S}^*)$$

And also

$$(\dot{S})^* = \left( \bigcap_{\sigma \in F} S^\sigma \right)^* = \sum_{\sigma \in F} (S^\sigma)^* = \sum_{\sigma \in F} (S^*)^\sigma = \overline{(S^*)}$$

And these identities work both for  $S \subset B/B^2$  and  $S \subset R$ . Now, we are looking for a group  $B_0$  of  $B$  in particular. This group has a special property: with the list of generators in our hands, we can check that it is invariant under conjugation by  $x$ . This means that  $x$  must fix the function whose square root generates the field, since the subspace duality is the Galois correspondence. Of the four functions  $\varphi, \varphi\psi_1, \varphi\psi_2, \varphi\psi_3$ , only  $\varphi$  is fixed by  $x$  (modulo squares). Therefore, the field we are looking for must be generated by a function  $Z$  such that

$$Z^2 = \varphi = \frac{(Y - \xi)(Y - \xi^2)}{(Y - \xi\sqrt[3]{2})(Y - \xi^2\sqrt[3]{2})}$$

Finally, the field  $\overline{\mathbb{Q}}(E_0)$  will be the normal closure of the extension  $\overline{\mathbb{Q}}(B_0)/\overline{\mathbb{Q}}(t)$ . This means adding all the Galois conjugates to  $Z^2$  (or taking the module generated by  $\varphi$ ). Since this module has dimension 4, it will be generated by the conjugates of  $\varphi$ . A basis is given by

$$\left\{ \begin{aligned} \varphi_1 = \varphi &= \frac{(Y - \xi)(Y - \xi^2)}{(Y - \xi\sqrt[3]{2})(Y - \xi^2\sqrt[3]{2})}; \varphi_2 = \varphi^{x^y} = \frac{(Y - 1)(Y - \xi)}{(Y - \sqrt[3]{2})(Y - \xi\sqrt[3]{2})}; \\ \varphi_3 = \varphi^y &= \frac{(X - \xi)(X - \xi^2)}{(X - \xi\sqrt[3]{2})(X - \xi^2\sqrt[3]{2})}; \varphi_4 = \varphi^{x^y y} = \frac{(X - 1)(X - \xi)}{(X - \sqrt[3]{2})(X - \xi\sqrt[3]{2})} \end{aligned} \right\}$$

Now, we can explicitly give the field of functions of the dessin  $E_0$ , which is a regular dessin whose field of moduli is not abelian. It is

$$\overline{\mathbb{Q}}(E_0) = \frac{\overline{\mathbb{Q}}(t)[X, Y, Z_1, Z_2, Z_3, Z_4]}{(t - (1 - (X^3 - 1)^2), X^3 + Y^3 - 2, Z_1^2 - \varphi_1, Z_2^2 - \varphi_2, Z_3^2 - \varphi_3, Z_4^2 - \varphi_4)}$$

The conjugate dessins are obtained by the action of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ : this means that they are built by taking the action of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  on the coefficients of the  $\varphi_i$ 's, which are the only functions involved with irrational coefficients. We can draw pictures of the ramification points of  $\overline{\mathbb{Q}}(B_0)/\overline{\mathbb{Q}}(B)$ , in order to visualize why the dessin  $E_0$  changes under the Galois action. In figure 3.7 we can mark the points where the extension is ramified, but  $E_0$  is the common cover (the intersection) of all six dessins conjugate to  $B_0$ , which means having  $\widehat{F}_2$  act on these points. For example, the action of  $y$  is a  $180^\circ$  rotation around  $(1, 1)$ , and it is not clear if we saw a picture of the rotated points whether they are conjugate to the same dessin. However, if we draw the universal cover of the dessin, which is  $\mathbb{C}$ , since the dessin has genus 1, we can visualize it a lot better, like in figure 3.8.

The fundamental domain is given by the two vectors, and the red points are the ones over which  $B_0$  ramifies. Now, if we imagine that  $(0, \sqrt[3]{2})$  is the biggest black point, the three hexagons around it make up the dessin as we have drawn it in figure 3.7. Now, the action of an element of  $\widehat{F}_2$ , such as  $y$ , can be lifted to this cover, as a rotation: if we take the  $y$  rotation, we are left with essentially the same image, and the effect is the same as changing the fundamental domain. This way, we can produce every dessin conjugate to  $B_0$ , and they are all within this image.

However, if we take the Galois action on the dessin  $B_0$ , the points over which it ramifies are also affected by the same action, and we are left with the pictures in figure 3.9.

These three are clearly not isomorphic to each other: there is no map that will preserve the red points. This just proves the fact that  $B_0$  is not fixed by the Galois action. It could be that its core,  $\cap_{g \in \widehat{F}_2} B_0^g$  was fixed, but it is not the case since we have proved it.

### 3.5 The field of moduli of the underlying curve

We have constructed the regular dessin given by the subgroup  $E_0 < \widehat{F}_2$ . This dessin corresponds to some Belyi pair  $(C, f)$ . We have also proven that when  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  doesn't fix  $\sqrt[3]{2}$ , the Belyi pair  $(C^\sigma, f^\sigma)$  is not isomorphic to  $(C, f)$ . However, it could be that the curves are isomorphic, i.e.  $C^\sigma \cong C$ . In this section, we are going to prove that this is not the case, so the field of moduli of the curve is also  $\mathbb{Q}(\sqrt[3]{2})$ .

The following is a sketch of the proof:

If the curves  $C$  and  $C^\sigma$  were isomorphic, then the curve  $C$  would have two regular dessins of the same degree. By a theorem of Wolfart [24], a curve with a regular dessin also has one unique regular dessin of maximum degree, which is given by the map  $C \rightarrow C/\text{Aut}(C)$ . We are going to prove that the dessin we have on  $C$  is already maximal, and therefore the curve cannot have more dessins of the same degree.

The way to do this is using the result in [6]: if a curve has a regular dessin given by the map  $C \rightarrow C/H$ , where  $H < \text{Aut}(C)$ , then the maximal dessin is given by doing the following: consider the dessin as a subgroup  $N$  of a triangle group  $\Delta_1$ . Then, the maximal dessin is given by including this  $\Delta_1$  in another triangle group

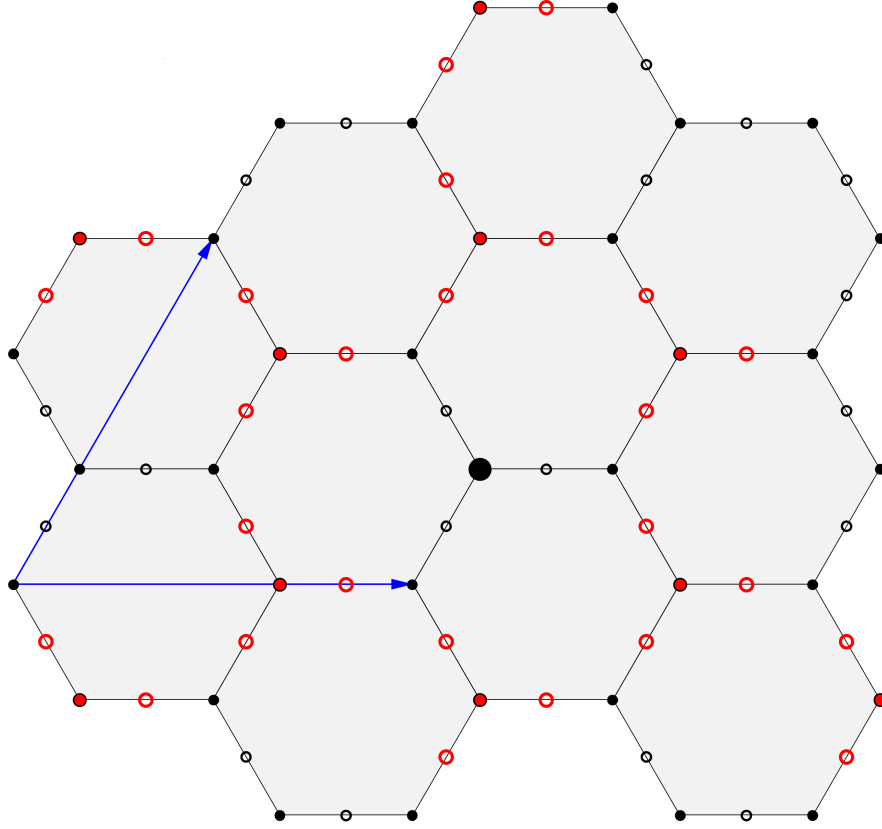


Figure 3.8: The universal cover of  $B$ , with the points where  $B_0$  ramifies marked in red.

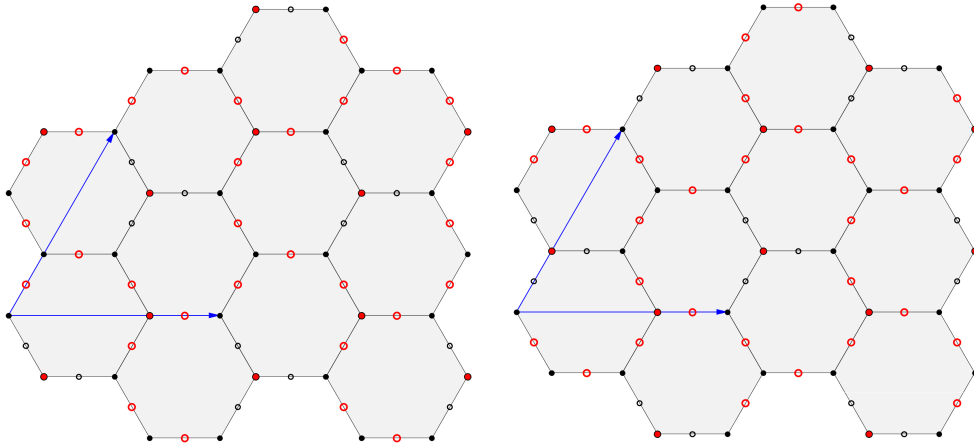


Figure 3.9: The universal cover of  $B$ , with the points where  $B_0^\sigma$  ramifies, where  $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \xi)/\mathbb{Q})$ .

$\Delta_2$  as a finite index subgroup. In order for the dessin obtained in this way to be regular,  $N$  must be a normal subgroup of  $\Delta_2$  under this inclusion. Our dessin is given in the triangle group  $\Delta(6, 4, 6)$ , which can only be included in  $\Delta(6, 8, 2)$  (the complete list of triangle group inclusions can be found in [22]). We prove that this inclusion doesn't make the subgroup of  $\Delta(6, 4, 6)$  normal in  $\Delta(6, 8, 2)$ , so the dessin we have must be of maximal degree.

Let us now talk about triangle groups and dessins with types. For a more detailed treatment of the subject, one can consult Wolfart's survey [24], section 2.2 in [9], or Gironde and González's textbook [7].

**Definition 3.5.1.** We say that a dessin, or a Belyi pair  $(C, f)$ , is of **type**  $(l, m, n)$  if the ramification order of every point in  $f^{-1}(0)$  divides  $l$ , the ramification order at  $f^{-1}(1)$  divides  $m$  and the ramification at  $f^{-1}(\infty)$  divides  $n$ .

In this definition, we are going to allow for some of  $l, m, n$  to equal  $\infty$ , with the convention that every number divides  $\infty$ . For example, every dessin is of type  $(\infty, \infty, \infty)$ .

In terms of drawings, this means that the order of every black vertex divides  $l$ , the order of every white vertex divides  $m$  and the number of sides on each face divides  $2n$  (if the ramification index at a point in the preimage of  $\infty$  is  $e$ , the corresponding face has  $2e$  sides:  $e$  that are oriented black-white in counterclockwise order and  $e$  in the opposite direction). In terms of the monodromy, since  $x$  takes the edges and makes them turn around black points, it means that  $x^l = 1$  in the cartographic group, and analogously, that  $y^m = 1$ . Since the action of  $z = (xy)^{-1}$  is turning around a face, it means that  $z^n = 1$ . Recall that the cartographic group is  $\widehat{F}_2/\text{Core}_{\widehat{F}_2} H$ , so the subgroup associated to the dessin contains the normal subgroup given by

$$N_{(l,m,n)} = \langle\langle x^l, y^m, z^n \rangle\rangle$$

Where the double brackets stand for the normal subgroup generated by the elements. Thus, by the correspondence between subgroups and dessins, dessins of type  $(l, m, n)$  are in correspondence with subgroups of finite index  $H$  such that  $N_{(l,m,n)} < H < \widehat{F}_2$ . Since the subgroups  $H$  are closed, they also contain the closure of  $N_{(l,m,n)}$ , which we will call  $\widehat{N_{(l,m,n)}}$ .

The closure of a normal subgroup is also normal, so the quotient  $\widehat{F}_2 \longrightarrow \widehat{F}_2/\widehat{N_{(l,m,n)}}$  is well-defined and we can give it the quotient topology, which will make it a profinite group, which we will call  $\Delta(l, m, n)$ . It is easy to check that it is the profinite completion of the group

$$\Delta(l, m, n) = F_2/N_{(l,m,n)}$$

Therefore, dessins of type  $(l, m, n)$  are in correspondence with open subgroups of  $\Delta(l, m, n)$ .

We are going to rely heavily on the uniformization theorem (which we have also used before, since it is used to prove that every compact Riemann surface is algebraic).

**Theorem 3.5.2** (Uniformization theorem). *There are only three simply connected Riemann surfaces, up to biholomorphism. They are*

- $\mathbb{P}^1$ , the Riemann sphere.
- $\mathbb{C}$ , the complex plane.
- $\mathbb{H} = \{z \in \mathbb{C} : \text{Re}(z) > 0\}$ , which is biholomorphic to the unit disc in  $\mathbb{C}$ .

Using this theorem, one can consider a compact Riemann surface  $C$  and its universal cover, which is also a Riemann surface and it is simply connected, so it will be one in the list. Then,  $C$  will be the quotient of one of these surfaces by the action of the fundamental group of  $C$ , which acts on the universal cover as biholomorphisms, and it does so properly and discontinuously. Studying the groups that act properly and discontinuously on these three surfaces, as it is done in [7], leads to concluding that the universal cover of a surface is  $\mathbb{P}^1$  if and only if the surface is the sphere, it is  $\mathbb{C}$  if it has genus 1, and it is  $\mathbb{H}$  if it has genus greater than 1.

If one has a regular dessin  $(C, f)$  of genus at least 2, one can consider the universal cover of  $C$ , which, as we have said, is  $\mathbb{H}$ . Then,  $C$  is the quotient of  $\mathbb{H}$  by the action of its fundamental group  $\Gamma$  (since the universal cover is a regular cover whose associated subgroup is 1). Let  $\pi$  be the projection from  $\mathbb{H}$  to  $\mathbb{H}/\Gamma$ .

**Lemma 3.5.3.** *Let  $C \cong \mathbb{H}/\Gamma$  be a curve of genus at least 2 and its universal cover. Then,  $\text{Aut}(C)$  lifts to  $N(\Gamma)$ , where  $N$  is the normalizer of  $\Gamma$  in the group of automorphisms of  $\mathbb{H}$ . That is, if  $\tilde{\varphi} \in N(\Gamma)$ , there exists some  $\varphi \in \text{Aut}(C)$  such that  $\pi \circ \tilde{\varphi} = \varphi \circ \pi$ , and reciprocally, if  $\tilde{\varphi} \in N(\Gamma)$ , then there exists some  $\varphi \in \text{Aut}(C)$  such that the identity holds.*

*This gives an isomorphism between  $\text{Aut}(C)$  and  $N(\Gamma)/\Gamma$ .*

*Proof.* We are going to prove that the automorphism group of  $C$ ,  $\text{Aut}(C)$ , lifts to  $\mathbb{H}$  inside of  $N(\Gamma)$ . Suppose we have an automorphism  $\varphi \in \text{Aut}(C)$ . We can consider  $\varphi \circ \pi : \mathbb{H} \longrightarrow C$ . This map will lift to  $\mathbb{H}$  by the lifting lemma, giving some  $\tilde{\varphi} : \mathbb{H} \longrightarrow \mathbb{H}$  such that  $\pi \circ \tilde{\varphi} = \varphi \circ \pi$ . This implies that  $\tilde{\varphi}$  will be invariant by the action of  $\Gamma$ , because, if we take some  $\gamma \in \Gamma$ , then,

$$\pi \circ \tilde{\varphi} \circ \gamma = \varphi \circ \pi \circ \gamma = \varphi \circ \pi = \pi \circ \tilde{\varphi}$$

Therefore,  $\tilde{\varphi}$  and  $\tilde{\varphi} \circ \gamma$  are liftings of the same map, so they must differ in the base point, and there must exist some  $\gamma' \in \Gamma$  that takes one base point to the other, so  $\gamma' \circ \tilde{\varphi} = \tilde{\varphi} \circ \gamma$ . Therefore,

$$\tilde{\varphi} \circ \gamma \circ \tilde{\varphi}^{-1} = \gamma' \in \Gamma$$

Which is what we wanted to prove: the lifting lies in  $N(\Gamma)$ .

Now for the reciprocal. Suppose  $\tilde{\varphi} \in N(\Gamma)$ . Then, for every  $\gamma \in \Gamma$ , there exists some  $\gamma' \in \Gamma$  such that  $\gamma' \circ \tilde{\varphi} = \tilde{\varphi} \circ \gamma$ . Therefore,  $\pi \circ \tilde{\varphi}$  is invariant under  $\Gamma$ : for any  $\gamma \in \Gamma$ ,

$$\pi \circ \tilde{\varphi} \circ \gamma = \pi \circ \gamma' \circ \tilde{\varphi} = \pi \circ \tilde{\varphi}$$

Therefore,  $\tilde{\varphi}$  is well-defined on the quotient  $\mathbb{H}/\Gamma$ , and it descends to some  $\varphi$  that will satisfy the required identity.

Note that an isomorphism  $\tilde{\varphi} \in N(\Gamma)$  descends to the identity if and only if it is in  $\Gamma$ . Therefore,  $\text{Aut}(C) \cong N(\Gamma)/\Gamma$ .  $\square$

This should not come as a surprise, since we have already proven that the automorphism group of a dessin is  $N_{F_2}(H)/H$ . By Hurwitz's automorphism theorem, the order of  $\text{Aut}(C)$  satisfies  $|\text{Aut}(C)| < 84(g-1)$ , and in particular, it is finite, and so is the index of  $\Gamma$  in  $N(\Gamma)$ .

Now, consider the dessin  $(C, f)$ . The map  $f$  induces another map  $f \circ \pi : \mathbb{H} \rightarrow \mathbb{P}^1$ . In Wolfart's paper [24] and in [7], it is proven that this map is of the form  $\mathbb{H} \rightarrow \mathbb{H}/\Delta$ , where  $\Delta$  is a triangle group.

The triangle groups in  $\text{Aut}(\mathbb{H})$  are defined as follows: take  $(l, m, n)$  such that  $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} < 1$  (if this is not the case, one can do the same in  $\mathbb{C}$  or  $\mathbb{P}^1$ , but we are working in the case where the genus is greater than 1). Then, construct in  $\mathbb{H}$ , with the hyperbolic metric, a triangle with angles  $2\pi/l, 2\pi/m, 2\pi/n$ . Such a triangle exists, since there are triangles with any angles provided their sum is less than  $2\pi$ . Take the group generated by the reflections on the sides of this triangle. If we call them  $a, b, c$ , then the triangle group is the index 2 subgroup generated by  $ab, bc, ca$ . It can be proven that this subgroup is isomorphic to the  $\Delta(l, m, n)$  we have already defined, and also that every two subgroups of  $\text{Aut}(\mathbb{H})$  isomorphic to the triangle group are conjugate in  $\text{Aut}(\mathbb{H})$  [7].

Suppose we have a regular dessin on a curve  $C = \mathbb{H}/\Gamma$  of type  $(l, m, n)$ , such that the ramification indices are precisely  $(l, m, n)$ . Let us prove that the corresponding  $\Delta$  is actually  $\Delta(l, m, n)$ : consider the unramified covers of  $C$ . When composed with the Belyi map on  $C$ , these covers also give covers of type  $(l, m, n)$ . Reciprocally, every cover of type  $(l, m, n)$  that covers  $C$  must be unramified over  $C$ , since, for any point  $P$  and any two functions  $f, g$ ,  $e_P(f \circ g) = e_{g(P)}(f)e_P(g)$ . Therefore, if we call  $U$  the universal cover of  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ , the subgroup of  $F_2$  associated to the covering  $U \rightarrow \mathbb{H}$  is precisely  $N_{(l, m, n)}$ . Also, suppose a regular dessin corresponds to a subgroup  $N \triangleleft F_2$ , so that the Belyi map is  $U/N \rightarrow U/F_2$ . Then, the map factors through  $U/N_{(l, m, n)}$ , since  $N \supset N_{(l, m, n)}$ . Then, we have the chain of coverings

$$U \rightarrow U/N_{(l, m, n)} \rightarrow U/H \rightarrow U/F_2 \cong \mathbb{P}^1$$

Also,  $U/H$  descends to  $U/N_{(l, m, n)}$  as the group  $\overline{H} = H/N_{(l, m, n)}$ , and the covering is then just

$$\mathbb{H}/\overline{H} \rightarrow \mathbb{H}/\Delta(l, m, n)$$

In Wolfart's paper [24], we have the following theorem (theorem 4).

**Theorem 3.5.4.** *Let  $C$  be a curve of genus at least 2. The following are equivalent:*

1.  $C$  has a regular dessin. We say that  $C$  is **quasiplatonic**.
2. When  $C$  is seen as the quotient of  $\mathbb{H}$  by the fundamental group  $\Gamma$  of  $C$ , there is some triangle group  $\Delta$  such that  $\Gamma < \Delta < N(\Gamma)$ .
3.  $N(\Gamma)$  is a triangle group.
4. The map  $C \rightarrow C/\text{Aut}(C)$  is a Belyi map (so  $\text{Aut}(C) \backslash C$  is isomorphic to  $\mathbb{P}^1$  and the map is ramified over at most three points).

Let us apply this to the curve in our example: the curve  $C$  that has the dessin given by the subgroup  $E_0 < \widehat{F}_2$ . Take  $\sigma \in \text{Gal}(\mathbb{Q}/\mathbb{Q})$  such that it doesn't fix  $\sqrt[3]{2}$ . If the conjugate curve  $C^\sigma$  was isomorphic to  $C$ , then  $C$  would have two different regular dessins: the one given by  $E_0$  and the one given by  $E_0^\sigma$ . Both of these are given by maps  $C \rightarrow C/H$ , where  $H$  is a subgroup of  $\text{Aut}(C)$ . By the theorem, it follows that there is a dessin of

maximum degree, given by  $C \rightarrow C/\text{Aut}(C)$ , and it must be unique. Therefore, if  $C^\sigma \cong C$ , the curve  $C$  must have another regular dessin, of greater degree than  $E_0$ .

We can see  $C$  as  $\mathbb{H}/\Gamma$ , so that the Belyi map  $f$  is  $\mathbb{H}/\Gamma \rightarrow \mathbb{H}/\Delta$ , where  $\Gamma < \Delta < N(\Gamma)$ . Now,  $(C, f)$  has type  $(6, 4, 6)$ , so the triangle group is  $\Delta(6, 4, 6)$ .

Therefore, we have that  $\Gamma < \Delta(6, 4, 6) < N(\Gamma)$ . If the dessin we are considering is not the regular dessin with the biggest degree, then  $N(\Gamma)$  must strictly contain  $\Delta(6, 4, 6)$ . Also, by the theorem, it is another triangle group. Now, Singerman [22] lists all the possible finite index inclusions between triangle groups, and [6] gives a list with inclusions that generate every inclusion. Looking at this list, we see that the only triangle group that contains  $\Delta(6, 4, 6)$  is  $\Delta(6, 8, 2)$ . If we give names to the generators so that

$$\Delta(6, 4, 6) = \langle x, y, z \mid x^6 = y^4 = z^6 = xyz = 1 \rangle$$

$$\Delta(6, 8, 2) = \langle \tilde{x}, \tilde{y}, \tilde{z} \mid \tilde{x}^6 = \tilde{y}^8 = \tilde{z}^2 = \tilde{x}\tilde{y}\tilde{z} = 1 \rangle$$

Then, the inclusion is given by

$$x = \tilde{x}$$

$$y = \tilde{y}^2$$

$$z = \tilde{z}\tilde{x}\tilde{z}$$

So  $\Gamma < \Delta(6, 4, 6) < \Delta(6, 8, 2)$  in this way, and it is clear that the inclusion between the triangle groups is of index 2. Now, the regular dessin given by  $E_0$  will be the maximal one, and therefore  $C \not\cong C^\sigma$ , if and only if  $\Gamma$  is not a normal subgroup of  $\Delta(6, 8, 2)$ . We will prove that this is the case.

As we said before,  $\Gamma$  is actually the group  $E_0/N_{(6,4,6)}$ . Therefore,  $\Gamma$  will be normal in  $\Delta(6, 8, 2)$  if and only if  $E_0/N_{(6,4,6)}$  is normal in  $\Delta(6, 8, 2)$ , with the inclusion written above.

$\Delta(6, 4, 6)$  is indeed normal in  $\Delta(6, 8, 2)$ , because it has index 2, so conjugation by elements of  $\Delta(6, 8, 2)$  gives an automorphism of  $\Delta(6, 4, 6)$ . We need to see if this automorphism fixes  $E_0/N_{(6,4,6)}$ .

Let us look at the action of the group by conjugation. In particular, let us look at the action of  $\tilde{y}$  (which we are choosing because it doesn't lie in  $\Delta(6, 4, 6)$ ). We have that  $\tilde{y}^{-1}y\tilde{y} = y^{\tilde{y}} = (\tilde{y}^2)^{\tilde{y}} = y$ . Also, Since  $\tilde{z} = (\tilde{x}\tilde{y})^{-1}$  has order 2,  $\tilde{x}\tilde{y} = \tilde{y}^{-1}\tilde{x}^{-1}$ , so

$$x^{\tilde{y}} = \tilde{y}^{-1}\tilde{x}\tilde{y} = \tilde{y}^{-1}\tilde{y}^{-1}\tilde{x}^{-1} = \tilde{y}^{-2}\tilde{x}^{-1} = y^{-1}x^{-1}$$

Therefore, the automorphism of  $E_0/N_{(6,4,6)}$  induced by  $\tilde{y}$  is given by

$$x \mapsto y^{-1}x^{-1}$$

$$y \mapsto y$$

Let us see if it fixes  $E_0$ . Take the subgroup  $F/N_{(6,4,6)}$ , which contains  $E_0$ . Recall that it is the normal subgroup generated by  $\{x^3, y^2, [x, x^y]\}$ . In particular, it is contained in the group  $A = \langle \langle x, y^2 \rangle \rangle$ , so  $E_0$  is also contained in this group.

Recall that  $E_0$  contained the element  $x^3(x^3)^y(x^3)^{y^2}$ . However, we are going to see that  $(x^3y^2(x^3y^2)^x(x^3y^2)^{x^2})^{\tilde{y}} \notin A$ . Indeed, we have that

$$(x^3y^2(x^3y^2)^x(x^3y^2)^{x^2})^{\tilde{y}} = (y^{-1}x^{-1})^3y^2((y^{-1}x^{-1})^3y^2)^{y^{-1}x^{-1}}((y^{-1}x^{-1})^3y^2)^{(y^{-1}x^{-1})^2}$$

And the word on the right contains an odd number of  $y$ 's, so it is not in  $A$ . Therefore,  $(x^3y^2(x^3y^2)^x(x^3y^2)^{x^2})^{\tilde{y}}$  isn't even in  $A$ , so it can't belong to  $E_0$ . Therefore,  $E_0$  is not normal in  $\Delta(6, 8, 2)$ , and we have proven that the dessin on  $C$  is the maximal one. Therefore, the curve  $C^\sigma$  is different from  $C$ .

We have thus found a quasiplatonic curve of genus 61 with field of moduli  $\mathbb{Q}(\sqrt[3]{2})$ .

### 3.6 A different example

Let us give another example of a regular dessin that has a field of moduli that is not abelian. Consider the following dessins which have the following sets of ramification indices: the points over 0 (the black vertices) have indices  $(2, 2, 1, 1)$ , the points over 1 have indices  $(3, 2, 1)$  and there is one point over  $\infty$  with index 6. In particular, its Euler characteristic is  $4 + 3 - 6 + 1 = 2$ , so the genus of the dessin is 0, and they are trees on  $\mathbb{P}^1$ .

Some fiddling around shows that there are three different dessins with these indices, namely the ones depicted in figure 3.10.



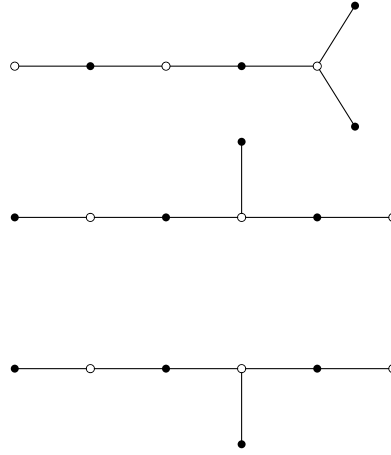


Figure 3.10: The three trees with vertex orders  $(2, 2, 1, 1)$ ,  $(3, 2, 1)$  and  $(6)$ .

Each of these dessins is given by a Belyi function  $f_i : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ , for  $i = 0, 1, 2$ . Since the only point in the preimage of  $\infty$  is  $\infty$ , the functions are actually polynomials. They are calculated in [21] (also in [20], and it is example 4.58 in [7]), and the formula for  $f_i$  is

$$f_i(z) = 1 - z^3(z+1)^2(z+a_i)$$

Where  $a_i$  runs through the roots of the irreducible polynomial

$$P = 25x^3 - 12x^2 - 24x - 16$$

It turns out that the roots of this polynomial are

$$a_0 = \frac{4 + 18\sqrt[3]{2} + 6\sqrt[3]{4}}{25}$$

And its conjugates

$$a_1 = \frac{4 + 18\xi\sqrt[3]{2} + 6\xi^2\sqrt[3]{4}}{25}$$

$$a_2 = \frac{4 + 18\xi^2\sqrt[3]{2} + 6\xi\sqrt[3]{4}}{25}$$

Where  $\xi^3 = 1$ .  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  permutes these roots, and therefore it induces a permutation of the three dessins. Also, their fields of moduli are  $\mathbb{Q}(a_i) = \mathbb{Q}(\xi^i\sqrt[3]{2})$ . If we call  $K = \mathbb{Q}(a_0, a_1, a_2) = \mathbb{Q}(\sqrt[3]{2}, \xi)$ , we have that  $\text{Gal}(K/\mathbb{Q}) \cong S_3$ . Thus, the Galois group of the extensions acts on the dessin as the usual action of  $S_3$  on three points.

Let us look at their regular covers, and prove that they are different. This will mean that, since the Galois action maps regular covers to regular covers, their fields of moduli are also  $\mathbb{Q}(a_i)$ .

We are going to see that the cartographic group is  $S_6$ . This can be found in [14], where a list of genus 0 dessins of degree up to 13 is given, along with their cartographic groups and their fields of definition.

Take their associated subgroups  $H_0, H_1, H_2 < \widehat{F}_2$ . The cartographic group is the image in  $S_6$  of the homomorphism  $\widehat{F}_2/\text{Core}_{\widehat{F}_2}(H_i) \rightarrow S_6$  induced by the action. For example, for a certain way of numbering the edges in figure 3.10, these maps are given by

	Top	Middle	Bottom
$x \mapsto$	$(14)(56)$	$(14)(26)$	$(14)(36)$
$y \mapsto$	$(123)(45)$	$(123)(45)$	$(123)(45)$

In every dessin, the permutation given by  $z = (xy)^{-1}$  is a cycle of order 6, since the exterior face has 6 edges, and  $y^3$  is a transposition, so together they generate the whole group  $S_6$ .

Let us call  $\overline{H}_i = \text{Core}_{\widehat{F}_2}(H_i)$ . Since the Galois group acts on these as the full permutation group, if two of them are equal, they are all equal. Suppose then that they are all equal. Take an element  $\sigma$  that has order three in  $\text{Gal}(K/\mathbb{Q})$ , so it permutes all three roots. For example, take the one that induces the permutation

$H_0 \rightarrow H_1 \rightarrow H_2$ . If  $\sigma$  fixed  $\overline{H_i}$ , then it would induce an automorphism of the quotient  $\widehat{F_2}/\overline{H_i}$ . This quotient is the cartographic group of the dessins, so it is isomorphic to  $S_6$ , for example by the isomorphism given by the monodromy of the first dessin. Furthermore, this automorphism is outer: it maps  $H_0/\overline{H_0}$ , which is the stabilizer of 1 by the action of  $S_6$ , to a subgroup  $H_1$ , that isn't conjugate to  $H_1$ , for if they were conjugate, the degree 6 dessins would be isomorphic.

However,  $\text{Out}(S_6)$  has order 2. Therefore,  $\sigma^4 = \sigma \in \text{Inn}(S_6)$  (for  $\sigma$  has order 3). This contradicts the possibility that  $\overline{H_0} = \overline{H_1} = \overline{H_2}$ , so these subgroups are different and they are interchanged by the Galois action. Therefore, their fields of moduli are  $\mathbb{Q}(a_i) = \mathbb{Q}(\xi^i \sqrt[3]{2})$ . Their genus is also 61, since their Euler characteristic is  $720 \cdot (1/2 + 1/6 + 1/6 - 1) = -120$ .

## References

- [1] BELYI, G. V., *On Galois Extensions of a Maximal Cyclotomic Field*, Mathematics of the USSR-Izvestiya 14 (2): 247, 1980
- [2] CONDER, M., JONES, G., STREIT, M., WOLFART, J., *Galois actions on regular dessins of small genera*, Rev. Mat. Iberoam. 28 (2012), no. 4, 1–19
- [3] COUVEIGNES, J.-M., *Calcul et rationalité de fonctions de Belyi en genre 0*, Ann. de l'Inst. Fourier, 994, vol. 44, no. 1, 1–38
- [4] COUVEIGNES, J.-M., *Dessins from a geometric point of view*, The Grothendieck theory of dessins d'enfants pp. 79–114, London Math. Soc. Lecture notes 200, Cambridge University Press, 1994.
- [5] FARKAS, H., KRA, I., *Riemann Surfaces*, Graduate texts in mathematics, Vol. 71, Springer, 1992
- [6] GIRONDO, E., *Multiply quasiplatonic Riemann surfaces*, Experimental Mathematics, Vol. 12, No. 4, 2003
- [7] GIRONDO, E., GONZÁLEZ-DIEZ, G., *Introduction to Compact Riemann Surfaces and Dessins d'Enfants*, London Mathematical Society Student Texts, Cambridge University Press, 2011
- [8] GIRONDO, E., GONZÁLEZ-DIEZ, G., *A note on the action of the absolute Galois group on dessins*, Bulletin of the London Mathematical Society, Vol. 39 Issue 5, p721, 2007
- [9] GONZÁLEZ-DIEZ, G., JAIKIN-ZAPIRAIN, A., *The absolute Galois group acts faithfully on regular dessins and on Beauville surfaces*, preprint, available at [http://www.uam.es/personal\\_pdi/ciencias/gabino/Jul03.pdf](http://www.uam.es/personal_pdi/ciencias/gabino/Jul03.pdf), 2013
- [10] GROTHENDIECK, A., *Esquisse d'un Programme*, 1984. It is published in Geometric Galois Actions. Around Grothendieck's Esquisse d'un Programme, edited by L. Schneps and P. Lochak, Cambridge University Press, 1997.
- [11] GUILLOT, P., *An elementary approach to Grothendieck's dessins d'enfants and the Grothendieck-Teichmüller group*, arXiv:1309.1968
- [12] HERFORT, W., RIBES, L., *Torsion elements and centralizers in free products of profinite groups*, Journal für die reine und angewandte Mathematik. Vol. 1985, 358, pp. 155–161
- [13] LANDO, S. K., ZVONKIN, A. K., *Graphs on Surfaces and their Applications*, Encyclopaedia of Mathematical Sciences: Lower-Dimensional Topology II 141, Berlin, New York, Springer-Verlag, 2004
- [14] MALLE, G., *Fields of definition of some three point ramified field extensions*, The Grothendieck theory of dessins d'enfants, London Math. Soc. Lecture notes 200, Cambridge University Press, 1994.
- [15] MIRANDA, R., *Algebraic curves and Riemann surfaces*, Graduate studies in mathematics, American Mathematical Society, 1995
- [16] MUNKRES, J., *Topology*, Prentice Hall, 2000
- [17] OSSERMAN, B., *Infinite Galois theory*, notes available at <https://www.math.ucdavis.edu/~osserman/classes/250C/>
- [18] RIVES, L., ZALESKII, P., *Profinite groups*, A Series of Modern Surveys in Mathematics, Springer-Verlag, 2000
- [19] SERRE, J. P., *Galois cohomology*, Springer, 2002
- [20] SCHNEPS, L., *Dessins d'enfants on the Riemann sphere*, The Grothendieck theory of dessins d'enfants, London Math. Soc. Lecture notes 200, Cambridge University Press, 1994.
- [21] SHABAT, G., VOEVODSKY, V., *Drawing curves over number fields*, The Grothendieck Festschrift, Progress in Mathematics Volume 88, 1990, pp 199–227
- [22] SINGERMAN, D., *Finitely maximal Fuchsian groups.*, J. London Math. Soc. (2) 6 (1972), 29–38.
- [23] WEIL, A., *The field of definition of a variety*, American Journal of Mathematics, Vol. 78, No. 3, 1956
- [24] WOLFART, J., *ABC for polynomials, dessins and uniformization - a survey*. Proceedings der ELAZ-Konferenz 2004, pp. 314–346 Hrsg. W. Schwarz, J. Steuding. Also available at <http://www.math.uni-frankfurt.de/~wolfart/>